الجمهورية العربية السورية
جامعة طرطوس
كلية هندسة تكنولوجيا المعلومات والاتصالات
قسم هندسة تكنولوجيا الاتصالات

زيادة تأثير العقد المهاجمة في تعطيل شبكات ad-hoc المعادية

دراسة أعدت لنيل درجة الماجستير في هندسة تكنولوجيا الاتصالات - قسم هندسة تكنولوجيا الاتصالات - كلية هندسة تكنولوجيا المعلومات والاتصالات

إعداد المهندس

محمد غسان علي

بإشراف

د. م. ناجي محمد (مشرف مشارك)

د . م . فادي غصّنه (مشرف رئيس)

2021

Syrian Arab Republic
Tartous University
Tartous University Journal
For Research and Scientific Studies
Established 2016
Tartous – SYRIA
Number/ Date:
Our Reference:

الجمهورية العربية السورية
جـــامعـة طـــرطـوس
مجلة جامعة طرطوس
للبحوث والدراسات العلمية
تأسست عام **2016**
طرطوس-سورية
الرقم / التاريخ : ٤٣٩ ٢٠٢١ / ٤-١٩ ٢٠٢١
الموضوع :

السيد الدكتور **فادي غصنه** المرتبة العلمية **أستاذ مساعد** في قسم **هندسة تكنولوجيا الاتصالات** من كلية **هندسة تكنولوجيا المعلومات والاتصالات** بجامعة **طرطوس**.

السيد الدكتور **ناجي محمد** المرتبة العلمية **مدرس** في قسم **هندسة تكنولوجيا الاتصالات** من كلية **هندسة تكنولوجيا المعلومات والاتصالات** بجامعة **طرطوس**.

السيد **محمد غسان علي** طالب دراسات عليا **(ماجستير)** في قسم **هندسة تكنولوجيا الاتصالات** من كلية **هندسة تكنولوجيا المعلومات والاتصالات** بجامعة **طرطوس**.

يسرنا إعلامكم أنه تمت الموافقة على نشر بحثكم المحكم المقدم للنشر في مجلة جامعة طرطوس للبحوث والدراسات العلمية ، وهو بعنوان :

دراسة تأثير هجوم الثقب الأسود على أداء بروتوكول التوجيه التفاعلي

AODV في شبكات MANET

في سلسلة **العلوم الهندسية** المجلد **(الخامس)** العدد **(الثالث)** لعام **2021** من مجلة جامعة طرطوس للبحوث والدراسات العلمية .

شكراً لاختياركم مجلتنا لنشر بحثكم ، وتفضلوا بقبول وافر التقدير

أمين التحرير

منار محمد عقول

رئيس جامعة طرطوس

الأستاذ الدكتور عصام محمد الدالي

الشكر والتقدير

عرفاناً بالجميل وتقديراً للجهد والعطاء يتقدم الباحث بأسمى آيات الشكر إلى مناهل العلم:

رئاسة جامعة طرطوس

كلية هندسة تكنولوجيا المعلومات والاتصالات "عمادة وهيئة تدريسية وإداريين"

واجب العرفان بالجميل يقتضي من الباحث أن يتقدم بجزيل الشكر والامتنان للسيدين:

الدكتور فادي جودت غصنه

الدكتور ناجي إبراهيم محمد

اللذان تفضلا بالإشراف على هذه الرسالة

كما يشكر الباحث عائلته وأصدقائه وكل من مدَّ يد العون لإنجاز هذا البحث

الملّخص

تُعتبَر شبكات الـ MANETs نظام اتصال لاسلكي هام جداً يقدم خدمات مستمرة لنقل البيانات بكفاءة عالية في بيئات يغيب فيها أي وجود لبنية تحتية (ذات البنية التحتية المدمرة كالشبكات العسكرية) نظراً للديناميكية التي تتمتع بها العقد من خلال تأسيس الاتصالات المباشرة، والتكيف السريع مع فقدان أي عقدة في الشبكة، لذلك تُعَد هذه الشبكات عرضة دائماً للتحديات الأمنية نتيجة محدودية الأمن الفيزيائي الذي تفرضه طبيعة وظروف عمل هذه النوع من الشبكات، يوجد الكثير من الأبحاث التي درست تأثير هجوم الثقب الأسود الأحادي على بروتوكول التوجيه التفاعلي AODV في شبكات ذات كثافة عقد متغيرة.

تم تطبيق هجوم انكار الخدمة على شبكات الـ MANET (Mobile Wireless Ad-hoc Network) حيث تمت دراسة تأثير هجوم الثقب الأسود (Black hole attack) بكلا نوعيه الفردي (Single) والتعاوني (Cooperative) على أداء بروتوكول التوجيه التفاعلي AODV في شبكات MANETs ضمن سيناريوهات متعددة لبيئات عمل متنوعة من حيث كثافة الشبكة وحركة العقد وعدد المهاجمين.

كلمات مفتاحية:

الشبكات النقّالة الخاصّة، الشبكات اللاسلكية متعددة القفزات، هجوم الثقب الأسود، بروتوكول AODV، البروتوكولات التفاعلية.

فهرس المحتويات

فهرس الأشكال

فهرس الجداول

المختصرات

الاختصار	المعنى باللغة الإنكليزية	المعنى باللغة العربية
MANETs	Mobile wireless Ad hoc Networks	الشبكات اللاسلكية متعددة القفزات
VANETs	Vehicle Ad hoc Networks	شبكات العربات المتحركة
WSNs	Wireless Sensor Networks	شبكات الحساسات اللاسلكية
WBSNs	Wireless Body Sensor Networks	شبكات حساسات الجسم اللاسلكية
AODV	Ad hoc On-demand Distance Vector	بروتوكول التوجيه المعتمد على شعاع المسافة عند الطلب
RREQ	Route Request	رسالة طلب المسار
RREP	Route Reply	رسالة إجابة المسار
RERR	Route Error	رسالة الخطأ
SIP	Source IP address	عنوان المصدر
DIP	Destination IP address	عنوان الهدف
SSN	Source Sequence Number	الرقم التسلسلي للمصدر
DSN	Destination Sequence Number	الرقم التسلسلي للهدف
PDR	Packet Delivery Rate	معدل وصول الرزم
ETD	End-To-end Delay	التأخير الزمني الكلي

معجم المصطلحات

المعنى باللغة العربية	المعنى باللغة الإنكليزية
هجوم الرجل في الوسط	Man-in-the Middle attack
الهجوم السلبي	Passive attack
الهجوم النشط	Active attack
هجوم إنكار الخدمة	Denial Of Service attack
هجوم الثقب الأسود الفردي	Single Black hole attack
هجوم الثقب الأسود التعاوني	Cooperative Black hole attack
هجوم الثقب الرمادي	Grey hole attack
هجوم الثقب الدودي	Worm hole attack
نماذج الأخطاء	Error modules
العقدة الخبيثة	Malicious node
العقدة الوسيطة	Intermediate node
عدد القفزات	Hop-counts
رسائل الترحيب	HELLO _ messages
زمن حياة المسار	Time To Life
شعاع المسافة	Distance Vector
الموثوقية	Authentication
عدم التنصل	Non-Repudiation
المصافحة الثلاثية	Three-way Handshake
اكتشاف المسار	Route Discovery
صيانة المسار	Route Maintenance
البروتوكولات الاستباقية	Proactive protocols
البروتوكولات التفاعلية	Reactive protocols
البروتوكولات الهجينة	Hybrid protocols

1 الفصل الأول

لمحة عامة عن البحث

1-1 المقدمة:

إن شبكات الـ (Ad-Hoc) هي مجموعة من العقد اللاسلكية التي تتصل مع بعضها البعض لاسلكياً باستخدام إشارات لاسلكية بواسطة قناة اتصال مشتركة، وكلمة Ad-Hoc تعني إن الأجهزة يمكن لها أن تنشئ اتصال في أي وقت وفي أي مكان دون مساعدة بنية تحتية مركزية وهذا هو المميز الأساسي لهذه الشبكات عن غيرها من أنوع الشبكات اللاسلكية، حيث تعمل العقد كموجهات وتكون قادرة على الحركة بحرية وبسرعات مختلفة وتُصنف هذه الشبكات ضمن أربع مجموعات أساسية وهي شبكة MANET (Mobile Wireless Ad Hoc Network)، وشبكة الحساسات اللاسلكية WSN (Wireless Sensor Network)، وشبكة VANET (Vehicle Ad Hoc Network)، وشبكة WBAN (Wireless Body Ad Hoc Network)، وتعاني هذه التقنية كغيرها من تقنيات الاتصال اللاسلكية من مشكلة محدودية الأمن الفيزيائي، وتكون الأجهزة المتحركة مسؤوله عن بناء وحفظ اتصالية الشبكة بشكل مستمر، وتتميز هذه الشبكات بعدة مواصفات وهي:

- عدم وجود إدارة مركزية.
- تتصل العقد مع بعضها البعض دون وجود بنية تحتية ثابته.
- يمكن لهذه الشبكات أن تتصل مع شبكات أخرى أو مع شبكة الانترنت.
- العقد ضمنها يمكن أن تكون مرسل أو مستقبل.
- تعمل أغلب هذه الشبكات على الحزمة الترددية المجانية .ISM (Industrial Scientific and Medical)

تجعل هذه الميزات هذه التقنية تؤمن الاتصال بين المستخدمين دون قيود، كما إنها تملك طوبولوجيا ديناميكية ومتغيرة باستمرار إذا كانت شبكة MANET لاسلكية متحركة وذلك نتيجة حركة العقد التي تؤدي إلى انقطاع الاتصال بينها وهذا يُعتَبر أمراً اعتيادياً في هذا النوع من الشبكات، وترتبط عناوين العقد بالأجهزة وليس بطوبولوجيا الشبكة حيث أن العناوين لا تدل على الموقع، ويُعَد التوجيه قضية هامة جداً ضمن شبكات MANETs وتنقسم بروتوكولات التوجيه إلى عدة أنواع هي البروتوكولات التفاعلية والاستباقية والهجينة [1].

وتتركز التطبيقات الأساسية لهذه الشبكات في تطبيقين أساسيين ألا وهما تبادل الملفات بين مجموعة من الأجهزة دون وجود عقدة مركزية (مشاركة الانترنت) وتبادل المعلومات لا توجد فيها بنية تحتية أو البنية التحتية تكون مدمرة (التطبيقات العسكرية)، ويبين الجدول التالي مقارنة بين الشبكات المخصصة Ad Hoc والشبكات الخلوية كما يلي:

Cellular networks	Ad Hoc network
تحتاج إلى بنية تحتية ثابتة	لا تحتاج إلى بنية تحتية ثابتة
شبكات ثابتة (محطات قاعدية)	لا يوجد محطات قاعدية
مواقع الخلايا تكون محددة مسبقاً وكذلك المحطات القاعدية	سريعة النشر
شبكات ذات طوبولوجيا عمود فقري ثابت	طوبولوجيا الشبكة ذات ديناميكية عالية
تحتاج إلى تخطيط مسبق قبل تنفيذ المحطات القاعدية	تتشكل أوتوماتيكياً وتتكيف مع التغيرات
بيئة مراقبة نسبياً واتصالية ثابتة	بيئة معادية واتصالية غير منتظمة
تكلفة اعداد عالية	تكلفة اعداد فعالة
زمن اعداد كبير	زمن اعداد منخفض

الجدول (1-1) مقارنة بين الشبكات الخلوية وشبكات Ad Hoc

وسوف تتركز دراستنا ضمن مجال الهجمات الأمنية لشبكات MANET حيث إنه في هذه الشبكات تتوضع العقد بشكل حر وشجري وبالنتيجة فإن طوبولوجيا الشبكة يمكن أن تتغير بشكل لحظي، سريع وعشوائي حيث إنها تتميز بطوبولوجيا ديناميكية، وبالإضافة إلى ذلك فأن هناك محدودية في الأمن الفيزيائي لهذه الشبكات حيث تعد مهددة كثيراً بالهجمات باعتبارها شبكات لاسلكية وذلك مقارنة مع الشبكات السلكية، وهو ما يعلل القيود والمحددات الفيزيائية التي تتحكم بالمعطيات المتنقلة عبر هذه الشبكات.

وسوف نقوم في هذه الأطروحة بتطبيق هجوم على الطبقة الثالثة (طبقة الشبكة Network Layer) باعتبارها الطبقة المسؤولة عن توجيه المعطيات من عقدة إلى أخرى، أي تعمل دائماً على إيجاد آلية توجيه فعالة لإيجاد أفضل مسار للبيانات. والهجوم الذي تم تنفيذه هو هجوم الثقب الأسود Black Hole Attack والذي سوف يتم استعراضه لاحقاً ضمن جسم هذه الأطروحة.

1-2 هدف البحث:

تركّزت أهداف البحث حول تحقيق النقاط التالية:

- تحسين إمكانية اختراق الشبكات المعادية.
- دراسة تأثير حركة العقد المهاجمة على سلوك الشبكة.
- تخفيض الإنتاجية وزيادة التأخير في الشبكات المعادية.
- دراسة الشبكة في حال وجود عقده مهاجمه واحده، في ظل كثافة متغيرة للشبكة.
- دراسة ومراقبة أداء الشبكة في حال وجود عدة عقد مهاجمه تعمل معاً.

1-3 مراحل البحث:

لقد مر البحث بعدة مراحل بدءً من اختيار بيئة العمل وتحديد هجوم للعمل علية وإيجاد الآلية المناسبة لتطبيق هذا الهجوم، ثم الانتقال إلى تحديد البنية الفيزيائية المناسبة للشبكة التي تم تطبيق الهجوم عليها وفق بروتوكول التوجيه المناسب، وانتقالاً إلى التطبيق الفعلي لهذا الهجوم على الشبكة وذلك وفق سيناريوهات هجوم متعددة ومختلفة من حيث كثافة الشبكة وعدد العقد المهاجمة ونماذج حركتها، ووصولاً إلى قياس بارامترات الأداء لهذه الشبكة واستخلاص أفضل الحالات لمهاجمة الشبكات المعادية.

1-4 طرق وأدوات البحث:

لقد أعتمد البحث أسلوب النمذجة والمحاكاة وفق برامج محاكاة معتمدة تستخدم في نمذجة ومحاكاة هذا النوع من الشبكات وتعتمد مبدأ محاكاة الأحداث المتقطعة وهي:

- NS3
- NS – 2.35
- OMNET++

1-5 الدراسات المرجعية:

سوف نقوم باستعراض الدراسات السابقة التي تطرقت إلى هجوم الثقب الأسود "Black hole attack" وذلك كما يلي:

في العام 2013 قام (khattak) بدراسة هجومي الثقب الأسود والرمادي"Black and Gray Hole attacks"، وتم اقتراح حل لهذا الهجوم في شبكات MANET، وذلك من خلال اختيار مسار سري لإرسال البيانات باتجاه الهدف، وهو ثاني أقصر مسار متوفر، ووُثق ذلك في الدراسة [2] بعنوان: " A Hybrid Approach for Preventing Black and Gray Hole Attacks in MANET ".

أقترح كل من (Deshmukh and Chatur) في العام 2016 حل لمشكلة هجوم الثقب الأسود من خلال استخدام التوجيه السري مع البروتوكول DSR، وذلك في حال وجود عقدة مهاجمة واحده أو عدة عقد مهاجمة تعمل معاً، وكان الحل المقترح هو تعديل بسيط على البروتوكول DSR من خلال إضافة العقدة الهدف بت تحقق(Validity bit) على رسالة الإجابة "RREP" قبل أن يتم إرسالها ضمن الشبكة، وبالتالي فإن كل عقدة وسطية سوف تتلقى هذه الرسالة

سوف تقوم بتفحص بت التحقق أولاً، وفي حال عدم تنصيبه سوف يتم حذف هذه الرسالة باعتبارها قادمة من عقدة مهاجمة، ويتم حظر العقدة المهاجمة التي أرسلت هذه الرسالة، وتم توثيق ذلك في الدراسة [3] بعنوان: "Secure Routing to Avoid Black Hole Affected Routes in MANET"

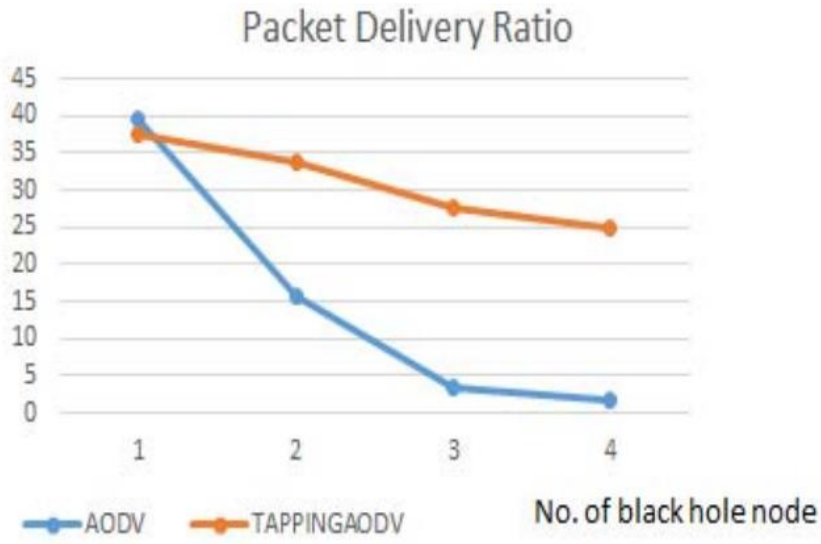
نُشرت في العام 2016 دراسة [4] بعنوان: "Hybrid Detection of Black hole and Gray hole attacks in MANET" قام بها الباحثان (Rathiga and Sathappan)، حيث اعتمدت هذه الدراسة على انتاج خوارزمية جديده للكشف ناتجة عن دمج خوارزميتين هما trust & collaborative Algorithms، وهاتان الخوارزميتان تقومان بكشف هجومي الثقب الأسود والرمادي، حيث اعتمدت الخوارزمية المقترحة على وضع عقد مراقبة (Monitor nodes) ضمن الشبكة هما العقدتان A و B، وتقوم هذه العقد بحساب شعاع المسافة (A,B) D_α لكل عقد الشبكة، ويتم وضع عتبات $\sigma 2, \sigma 1$، وعند تجاوز هذه العتبات تعتبر العقدة عقدة خبيثة ويتم استبعادها.

قام الباحثان (Sharma and Bisen) في العام 2016 بدراسة بعنوان: "Detection As Well As Removal Of Black hole And Gray hole Attack In MANET"، خلصت هذه الدراسة إلى إيجاد خوارزمية لاكتشاف ومنع هجومي الثقب الأسود والرمادي في شبكات MANET، [5] واعتمدت هذه الخوارزمية في عملها الشبكات العاملة وفق البروتوكول AODV، وسُميَت "Trap AODV"، وتعتمد هذه الخوارزمية في مبدأ عملها على مرحلتين وهما: مرحلة اكتشاف المسار"Route Discovery phase"، ومرحلة مراقبة الجيران "Monitoring phase".

حيث أنه خلال المرحلة الأولى (اكتشاف المسار) تقوم العقدة المصدر بإرسال رسالة طلب مسار RREQ وهمية على شكل فخ، لأنها تحوي عنوان ID لعقدة بالأصل غير موجودة ضمن الشبكة، وطبعاً سوف تقوم العقد الخبيثّة بإرسال رسالة الإجابة RREP رداً على طلب المسار، وبالتالي سوف تكتشف العقدة المصدر أن العقدة التي أرسلت الإجابة هي عقدة مهاجمة، وتقوم بإرسال رسالة تنبيه لكل العقد ضمن الشبكة لإعلامهم بوجود العقدة المهاجمة ليتم استبعادها من المشاركة في انشاء المسارات، وبعد ذلك يتم ارسال رسالة طلب مسار حقيقية واذا كانت الشبكة لاتزال تحوي عقد مهاجمة سيتم اكتشافهم في المرحلة التالية وهي مرحلة المراقبة "Monitoring phase".

في مرحلة مراقبة الجيران تقوم كل عقدة بمراقبة معدل التوجيه لجيرانها، علماً أنه يجب ألا تقل قيمته عن عتبة معينة محددة مسبقاَ، فإذا كان هذا المعدل أقل من العتبة سوف تقوم العقدة المراقِبة بإعلام العقدة المصدر بذلك، ليقوم المصدر بإضافة العقدة المهاجِمة إلى قائمة العقد المهاجمة، ويقوم بإرسال رسالة تنبيه إلى كل عقد الشبكة على شكل بثّ عام لإعلامهم بوجود عقدة مهاجمة، وبعد ذلك يتم من جديد إرسال رسالة طلب المسار.

تم في هذه الدراسة قياس معدل وصول الرزم PDR (Packet Delivery Ratio)، حيث تمت المقارنة بين أداء البروتوكول المقترح Trap AODV والبروتوكول AODV الأساسي وذلك عند تغير عدد العقد المهاجمة ضمن الشبكة، وكانت النتيجة تفوق البروتوكول المقترح كما يلي:



الشكل(1−1) قياس معدل وصول الرزم PDR

نُشرت دراسة قام بها الباحث (Thakker) عام 2016 بعنوان: "Avoidance of Co−operative black hole attack in AODV in MANET"، حيث اقترح الباحث آلية لاكتشاف وحّل هجوم الثقب الأسود في شبكات MANET العاملة مع البروتوكول AODV، [6] سواء أكان هجوم من عقدة مهاجمة واحدة أو عدة عقدة مهاجمة تعمل معاً (master & slaves)، حيث اعتمدت خوارزمية الكشف على تحديد قيمة عتبة ثقة (trust value) تحسب وفق قانون محدد:

$$T = tanh(R_1 + R_2 + A)$$

حيث:

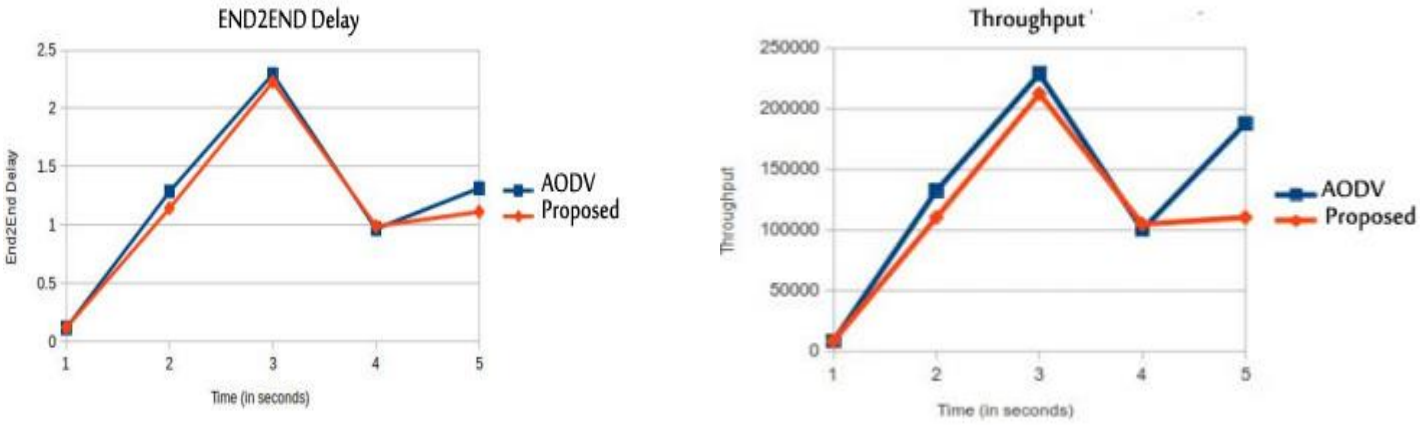
R_1 : هي نسبة الرزم المستقبلة إلى الرزم المرسلة من قبل العقدة.

R_2 : هي نسبة عدد رسائل طلب المسار المستقبلة إلى عدد رسائل الإجابة المرسلة من قبل العقدة.

A : هو بت التحقق (Acknowledge bit).

واعتمدت آلية الكشف في الخوارزمية المقترحة أنه عندما تتلقي أي عقدة في الشبكة أي رسالة فالخطوة الأولى تكون تفحص نوعها هي رسالة إجابة أم رسالة بيانات، فإذا كانت الرسالة المستقبلة هي رسالة إجابة تقوم العقدة بحساب العتبة T_1 للعقدة المُرسِلة، وإذا كانت هذه العتبة أقل من العتبة المحددة مسبقاً فإن مصدر الرسالة يُعتبَر عقدة مهاجمة وبالتالي يتم حذف هذه الرسالة، وإلا يتم الانتقال إلى حالة المعالجة الطبيعية للبروتوكول AODV.

تمت المقارنة بين أداء البروتوكول AODV القياسي والخوارزمية المقترحة من خلال قياس الإنتاجية (throughput) والتأخير الزمني (Delay) وتم الحصول على النتائج التالية:



(ب) (أ)

الشكل(1-2): (أ) قياس الإنتاجية، (ب) قياس التأخير الزمني

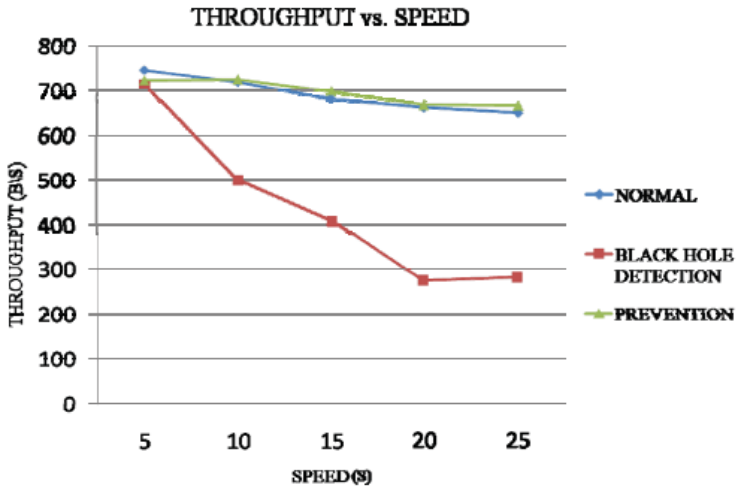
نلاحظ حسب الشكل(1-2) وجود حالة تطابق تقريباً بين الخوارزمية المقترحة للكشف والحالة القياسية لبروتوكول التوجيه AODV.

وفي العام 2016 قام (Nitnaware) باقتراح استراتيجية لاكتشاف الهجوم في شبكات MANET [7]، واعتمدت الخوارزمية المقترحة على البروتوكول DYMO (Dynamic MANET On demand) وهو بروتوكول تفاعلي متعدد القفزات، ويُعَد تطوير للبروتوكول AODV، ويعتمد هذا البروتوكول على استخدام ثلاث أنواع من الرسائل في إيجاد المسار المتاح باتجاه الهدف، وهي رسالة طلب المسار RREQ، ورسالة الإجابة RREP، ورسالة الخطأ RERR (Route error)، والتي تُستخدَم عند حدوث مشكلة في الوصلة.

اعتمدت الخوارزمية المقترحة على إضافة وحدة مدمجة BDS وظيفتها حساب قيمة مشبوهة (suspicious value) تتعلق هذه القيمة بقدرة أو طاقة الإرسال (transmission power)، وارتفاع الهوائي، وتُحسب هذه القيمة لكل العقد ضمن الشبكة، وذلك عن طريق ارسال رسائل Hello التي تطلب معلومات عن العتاد الصلب (طاقة البطارية وارتفاع الهوائي).

وإذا تجاوزت القيمة المشبوهة التي يتم حسابها (Tr power) لعقدة جارة ما قيمة العتبة المحددة يتم عزلها من الشبكة، وبالتالي فإن العقد الأخرى لن تقوم بتوجيه البيانات عبرها لأنها عقدة خبيثّة، وذلك على اعتبار أن الطاقة العظمى لكل العقد ضمن الشبكة محددة ومعلومة مسبقاً.

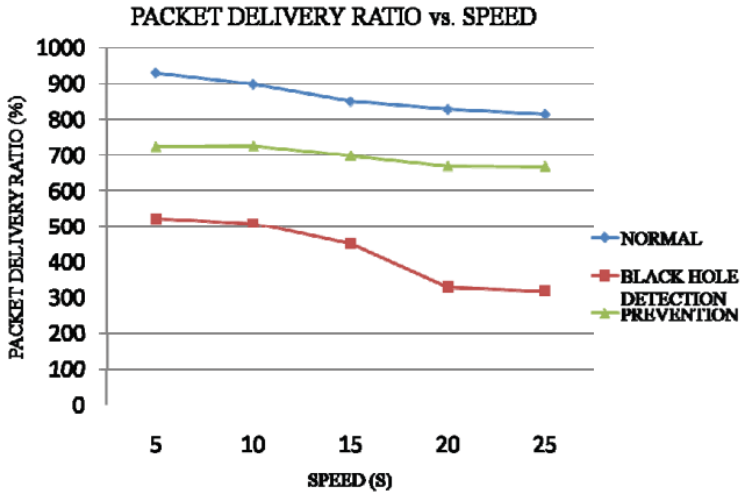
قام الباحث بالمقارنة بين ثلاث حالات للبروتوكول وهي حالة عدم وجود عقد مهاجمة، وحالة وجود عقد مهاجمة، وحالة حل واكتشاف العقد المهاجمة، وتم قياس الإنتاجية (throughput)، ومعدل وصول الرزم (PDR)، وذلك عند تغّير سرعة العقد (الحركية) ضمن الشبكة وكانت النتائج كما يلي:



الشكل(1-3): قياس الإنتاجية مع تغير السرعة

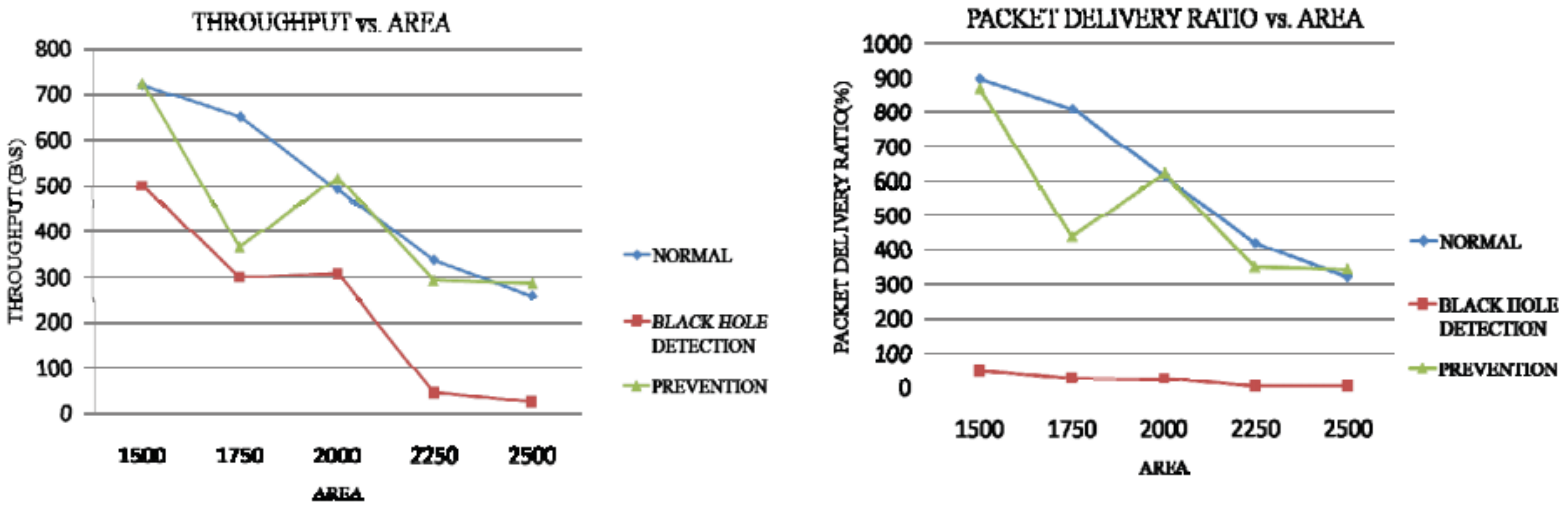
تظهر المخططات فعالية الخوارزمية المقترحة حيث إنها تطابق الحالة القياسية للبروتوكول تقريباً، وأيضاً نلاحظ أن قيمة الإنتاجية تتناقص عن زيادة سرعة العقد ضمن الشبكة.

أما بالنسبة لمعدل إيصال الرزم PDR كانت النتائج كما يلي:



الشكل(1-4): قياس معدل وصول الرزم مع تغير السرعة

نلاحظ أيضاً فعالية الخوارزمية المقترحة واقترابها من الحالة القياسية للبروتوكول، وأيضاً زيادة معدل إيصال الرزم بزيادة عدد العقد ضمن الشبكة، في حين تنخفض قيمته عند زيادة السرعة وذلك عند عدد ثابت للعقد المكّونة للشبكة، أيضا تم قياس الإنتاجية ومعدل وصول الرزم وذلك عند تغير مساحة منطقة العمل (مساحة الشبكة) ولاحظنا حدوث انخفاض كبير في هاتين القيمتين، حيث يزداد هذا الانخفاض بزيادة مساحة الشبكة كما يلي:



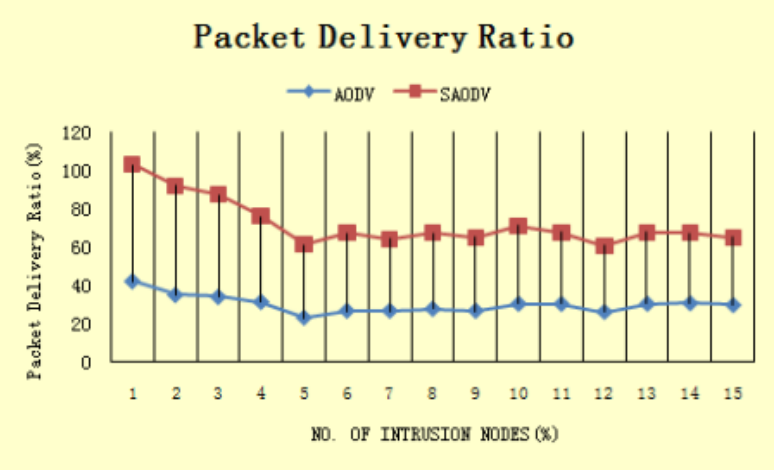
(ب) (أ)

الشكل(1-5): (أ) قياس الانتاجية مع تغير السرعة، (ب) قياس معدل وصول الرزم مع تغير السرعة

في العام 2017 قام الباحثون (Saurabh, Sharma, Itare and Singh) بإيجاد تقنية لاكتشاف ومنع هجوم الثقب الأسود في شبكات MANET [8]، واعتمدت هذه التقنية في عملها على مبدأ العناقيد، حيث تم تقسيم عقد الشبكة إلى عدة أجزاء هي عبارة عن عناقيد (Clusters)، وكل عنقود يكون له قائد عنقود وهو عبارة عن عقدة يتم اختيارها بشكل عشوائي، ويقوم قائد العنقود بالإعلان عن نفسه لعقد الجوار، وبعد ذلك تقوم العقد بفحص اتصالها مع قادة العناقيد وذلك بعملية "ping".

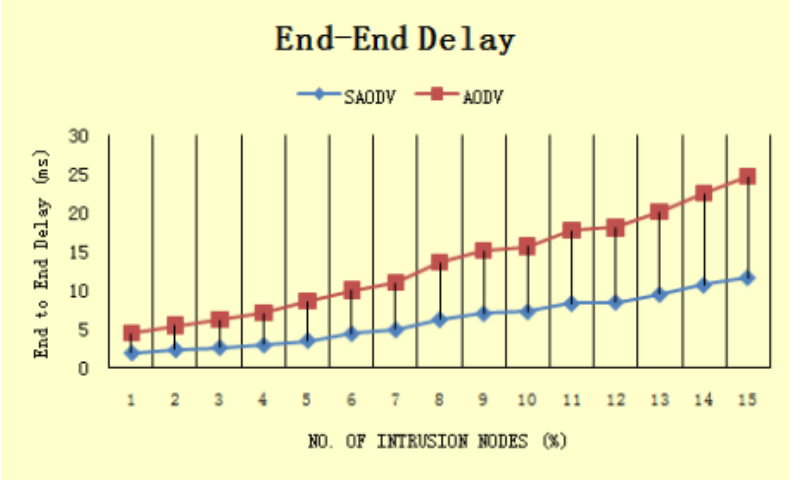
إن كل قائد عنقود هو عبارة عن نقطة اختبار (check-point) مهمته حساب النسبة N_d/N_s لكل عقدة ضمن عنقوده، وتعرف هذه النسبة بمعدل التوصيل P_d، ويجب أن تكون أكبر من عتبة محدده T حتى تكون هذه العقدة عقدة طبيعية ضمن الشبكة، أما اذا كانت $P_d < T$ ففي هذه الحالة يتم الاشتباه بالعقدة إنها عقدة مهاجمة، فاذا كانت نسبة الرزم التي تقوم بإسقاطها تتجاوز 20 % من الرزم الكلية المرسلة بواسطة العقدة المصدر عندئذ فإن العقدة المصدر سوف تقوم بإرسال الرزمة التالية من البيانات فقط عند تلقي إشعار الوصول من الهدف، وقد تم توثيق هذه التقنية في الدراسة التي نُشرت بعنوان: "Cluster-based Technique for Detection and Prevention of Black-Hole Attack in MANETS".

إن الخوارزمية المقترحة (SAODV) حققت نتائج مهمة جداً مقارنة مع الحالة الطبيعية للبروتوكول (AODV) وذلك كما يلي:



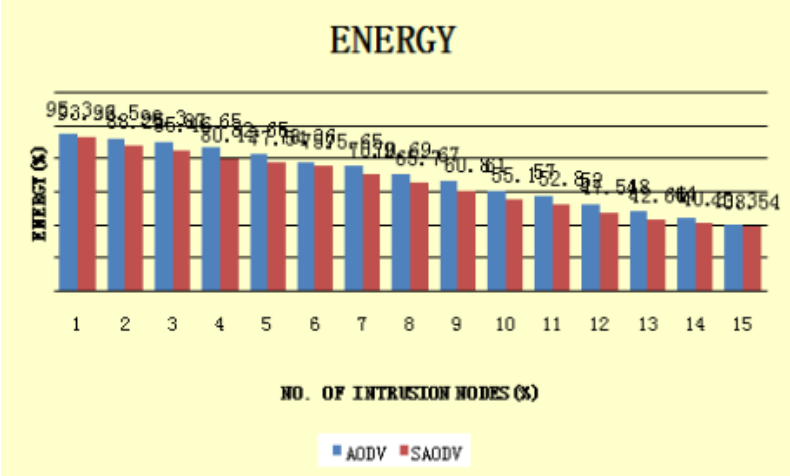
الشكل(1-6): قياس معدل وصول الرزم مع تغير الكثافة

حيث نلاحظ تحسن كبير جداً في معدل إيصال الرزم (PDR) وهذا التحسن حوالي ثلاث أضعاف، وأيضا تقليل التأخير الزمني (delay)، علماً أن كل النتائج أُخذت في حالة المتوسط (average)، وذلك كما هو مُوضَح في الشكل(1-6) التالي:



الشكل(1-7): قياس التأخير الزمني مع تغير الكثافة

كما أن البروتوكول المُقترح يستهلك طاقة (energy) أقل من البروتوكول AODV بحالته الطبيعية، كما هو مُوضّح في الشكل(1-7) التالي:



الشكل(1-8): قياس الطاقة مع تغير الكثافة

هدف كل من (Dhende and Musale) في العام 2017 في الدراسة التي نُشرت بعنوان: "SAODV: Black Hole and Gray Hole Attack Detection Protocol in MANETs" إلى إيجاد خوارزمية تعتمد بشكل كامل على الجيران في تحديد نوع العقد ضمن الشبكة (طبيعية أو مهاجمة)، وسُميت هذه الخوارزمية SAODV والتي اعتمدت في مبدأ عملها بشكل على عنصرين أساسيين وهما قائمة الجيران (N_L) neighbor's list، وجدول الرأي opinion table (O_T).

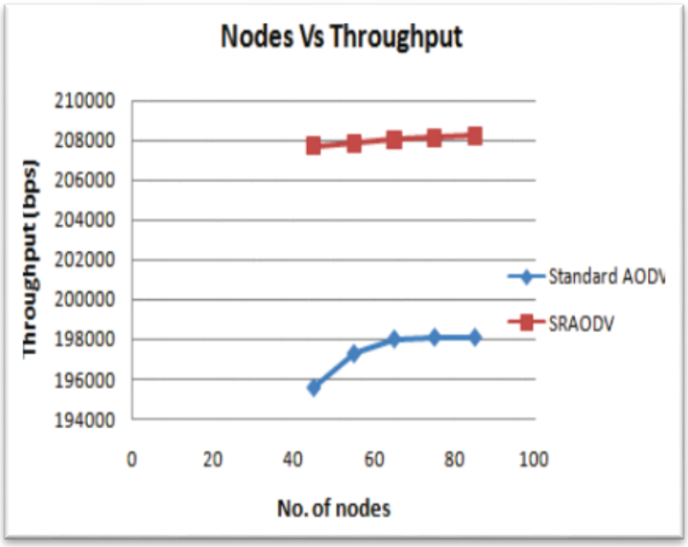
حيث إن كل العقد ضمن الشبكة تقوم وبشكل دوري بتخزين معلومات عن جيرانها، وهذه المعلومات تكون مخزنة ضمن جدولين صغيرين، الجدول الأول هو قائمة الجيران (N_L) والذي يحوي على معرفات العقد (IDs) لكل الجيران ويتم تحديثه دورياً، والجدول الثاني هو جدول الرأي (O_T) والمسؤول عن تحديد نوع العقدة فيما إذا كانت عقدة طبيعية أم عقدة خبيثّة (مهاجمة هجوم ثقب أسود أو رمادي) [9].

وآلية عمل الخوارزمية المقترحة تكون كما يلي: عندما تريد عقدة ما (مصدر) إرسال بيانات إلى عقدة أخرى (هدف) فأنها ستقوم بتفعيل إجرائية طلب مسار RREQ، وتنتظر استقبال رسائل الإجابة RREP، وبعد استلام رسائل الإجابة يقوم المصدر بإرسال رسالة على شكل بث عام يسأل فيها العقد الجيران عن رأيهم بالعقدة المجيبة (هل هي خبيثّة؟)، فيقوم الجيران بالإجابة بنعم أم لا وذلك من خلال إرسال رسائل (YES) أو (NO)، وبعد ذلك يقوم المصدر بتجميع هذه الرسائل وفحصها.

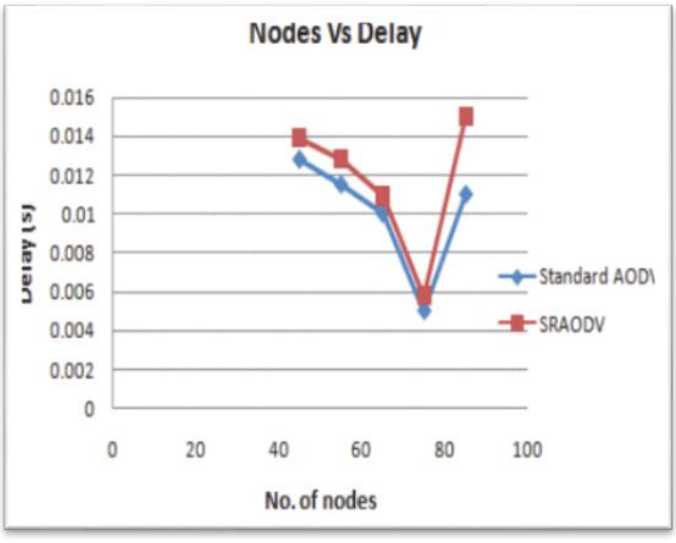
فإذا كانت كل الإجابات (YES) فإن العقدة المجيبة هي عقدة مهاجمة هجوم ثقب أسود ويجب حظرها واستبعادها من الشبكة وتنبيه باقي عقد الشبكة، أما اذا تباينت الإجابات بين (YES) و (NO) فإن العقدة مهاجمة هجوم ثقب رمادي

وأيضاً يتم استبعادها، وفي خلاف ذلك أي اذا كانت كل الإجابات (NO) فإن العقدة المجيبة هي عقدة طبيعية ويتم ارسال البيانات لها بشكل طبيعي.

تمت المقارنة بين البروتوكول المقترح (SRAODV) مع البروتوكول المعياري (standard AODV)، ونلاحظ أنه تم تحقيق تحسين كبير بالإنتاجية، ولكن بالمقابل حصلت زيادة طفيفة في التأخير الزمني وذلك وفق الشكليين(1-8) و(1-9) التاليين:



الشكل(1-9): قياس الإنتاجية مع تغير الكثافة



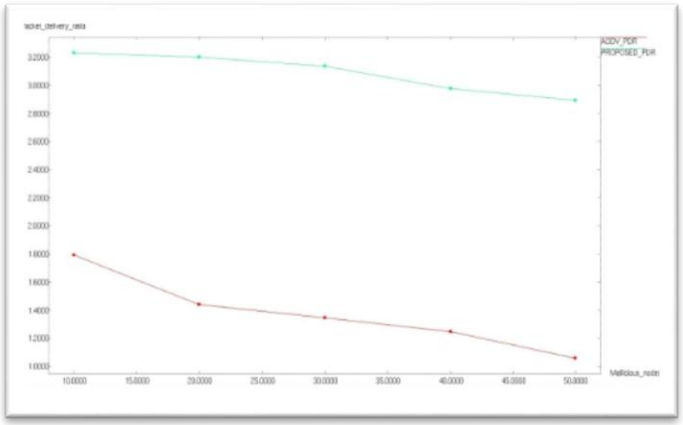
الشكل(1-10): قياس التأخير الزمني مع تغير الكثافة

نفذَ الباحثان (Panda and Pattanayak) في عام 2018 خوارزمية لاكتشاف ومنع الهجوم في شبكات MANET، وسُمي البروتوكول المقترح EAODV، حيث حسنت الخوارزمية المقترحة أداء الشبكة، لكنه أيضاً نتج عنها زيادة واضحة في حمل التوجيه (routing overhead) ضمن الشبكة، وهذا يظهر بشكل واضح مع زيادة عدد المهاجمين، واعتمدت الخوارزمية المقترحة في مبدأ عملها على استخدام التوقيع الرقمي لمنع هجوم الثقب الأسود الداخلي والخارجي، وبالتالي فإن كل عقدة تدخل الشبكة سوف تُعطى مفتاح خاص (private key) ومفتاح عام (public key) وذلك من أجل إمكانية التوقيع الرقمي، وكل عقدة تقوم باكتشاف جوارها عن طريق تبادل رسائل Hello.

حيث إنه عندما تريد العقدة المصدر إرسال بيانات لعقدة ما فإنها تقوم بإرسال رسالة Forward Agent(FA)، وكل عقدة تصلها هذه الرسالة سوف تقوم أولاً بالاطلاع عليها والتحقق منها وذلك عن طريق استخدام المفتاح الخاص (private key) لفك تشفيرها، وتستمر هذه الآلية وصولاً إلى العقدة الهدف والتي تقوم بدورها بالتحقق من الرسالة بالإضافة الى إنهاءها، ثم تقوم بتوليد رسالة جديدة هي رسالة إجابة Backward Agent(BA) تسلك المسار العكسي وصولاً إلى المصدر، وبذلك يكون المسار قد تم تأسيسه وتبدأ بعدها عملية إرسال البيانات [10].

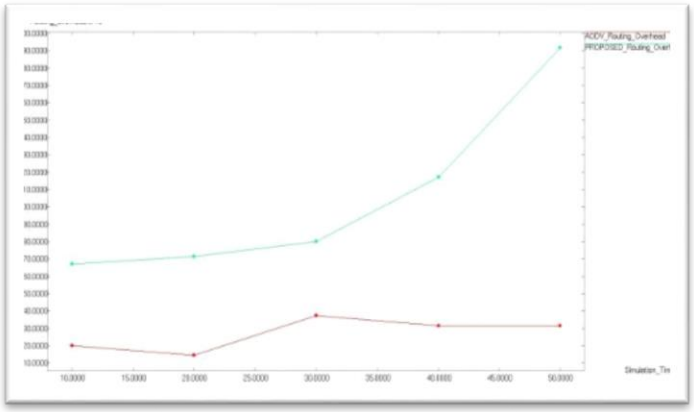
وعند اكتشاف أي خطأ في رسائل FA أو BA من قبل أي عقدة وسيطيه، يتم التعامل معه من خلال حذف الرسالة مباشرة من قبل العقدة التي اكتشفت الخطأ، وبذلك يتم حل مشكلة الهجوم الخارجي، بالإضافة إلى ذلك فإنه خلال مرحلة تبادل البيانات تقوم كل عقدة بمراقبة معدل التوجيه لجيرانها ليتم اكتشاف أي مهاجم داخلي في حال وجوده، وقد تم توثيق هذه الخوارزمية في الدراسة التي نُشرت بعنوان: "Energy aware detection and prevention of black hole attack in MANET".

تظهر عملية المقارنة بين الخوارزمية المقترحة والبروتوكول المعياري AODV فعالية كبيرة للتقنية المقترحة، من خلال قياس معدل وصول الرزم الموضح بالشكل (1-11).



الشكل(1-11) معدل وصول الرزم

بالإضافة إلى ذلك حققت الخوارزمية المقترحة استهلاك فعّال للطاقة، ولكن بالمقابل نلاحظ وجود حمل توجيه كبير ضمن الشبكة ناتج عن تبادل عدد كبير من الرسائل وذلك من خلال قياس حمل التوجيه (routing overhead) كما يلي:



الشكل(1-12) حمل التوجيه "Routing Overhead"

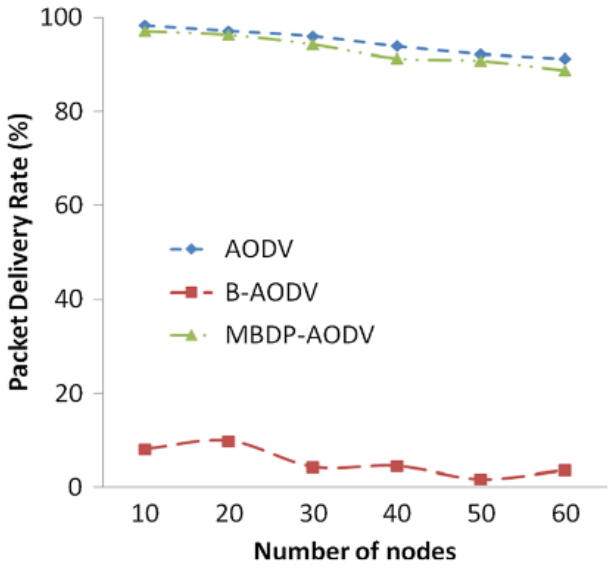
في العام 2019 قام الباحثان (Shashi and Siddhartha) باقتراح وتنفيذ خوارزمية تعتمد على حساب قيمة عتبة ديناميكية لحل مشكلة هجوم الثقب الأسود في شبكات MANET [11]، وسميت MBDP-AODV، حيث تم الاعتماد على حساب قيمة العتبة المتغيرة للكشف على الرقم التسلسلي SN للهدف والذي يكون مضمناً في رسالة الإجابة، علماً أن التقنية المقترحة لا تحتاج إلى أن تكون العقد في وضع المراقبة، وتعمل هذه الخوارزمية وفق ثلاث مراحل وهي مرحلة حساب العتبة ومرحلة الكشف ومرحلة المنّع.

في مرحلة حساب العتبة يتم حساب المتوسط والانحراف المعياري للأرقام التسلسلية لرسائل الإجابة (RREP) الواصلة للمصدر، حيث إن قيمة الانحراف المعياري الناتجة هي قيمة العتبة التي يتم اعتمادها.

بعد حساب العتبة يتم الانتقال إلى المرحلة التالية وهي مرحلة الكشف، حيث يقوم المصدر بإرسال رزمة بيانات تحوي الرقم التسلسلي المشتبه به، وبالتالي أي عقدة تحتوي هذا الرقم التسلسلي ولها عدد قفزات يساوي الواحد تُعتبر عقدة مهاجمة وبذلك يتم كشفها، ثم يتم الانتقال إلى المرحلة التالية وهي مرحلة المنع حيث يتم في هذه المرحلة إرسال رسالة تنبيه لكل عقد الشبكة تحتوي عنوان معرف العقدة المهاجمة "ID" لتقوم كل العقد بإضافتها إلى قائمة العقد الخبيثّة، وبالتالي أي رسالة مصدرها العقدة المهاجمة يتم حذفها مباشرة.

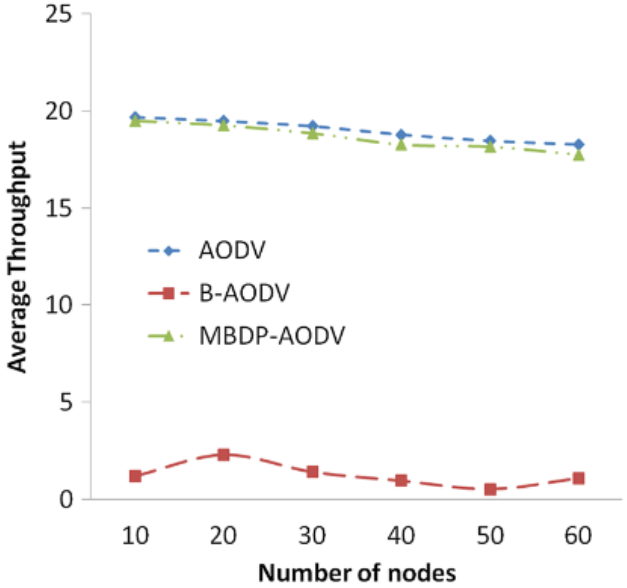
تم توثيق هذه الخوارزمية في الدراسة التي نُشرت بعنوان: "A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET".

حققت الخوارزمية المقترحة كفاءه عالية ونلاحظ ذلك من خلال حالة التطابق بين الحل المقترح والحالة الطبيعية للبروتوكول AODV وذلك في حساب كل من الإنتاجية ومعدل وصول الرزم كما يلي:



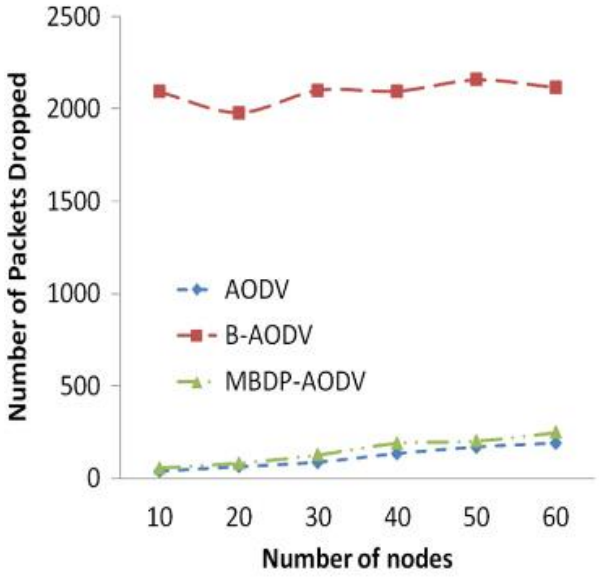
الشكل(1-13) معدل وصول الرزم PDR

وأيضاً

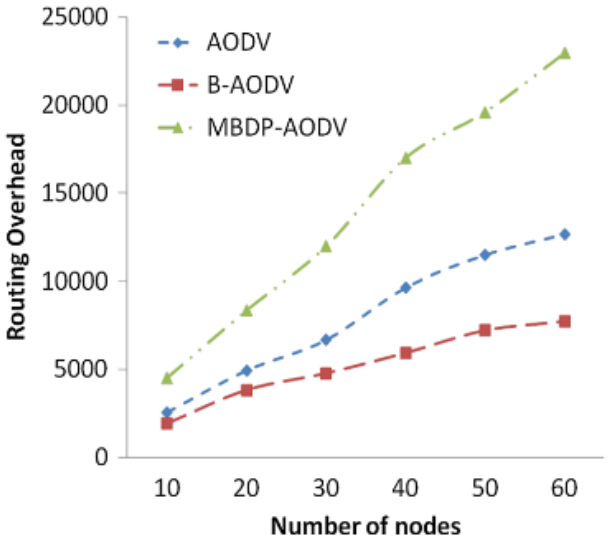


الشكل(1-14) الإنتاجية Throughput

نلاحظ أيضاً وجود معدل ضياع منخفض جداً ويوافق الحالة الطبيعية، لكن بالمقابل انتجت حمل توجيه (routing overhead) مرتفع بشكل ملحوظ ضمن الشبكة كما يلي:



الشكل(1-15) معدل ضياع الرزم



الشكل(1-16) حمل التوجيه Routing Overhead

2 الفصل الثاني

الأنواع الرئيسية لشبكات Ad Hoc

(VANETs–WSNs–MANETs–WBSNs)

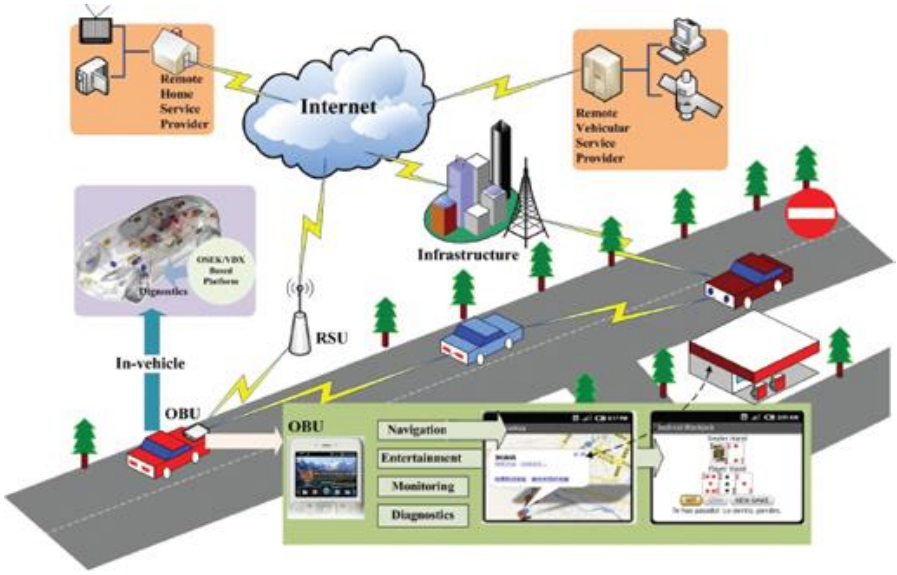
تُقسَم الشبكات النقّالة الخاصة "Ad hoc" إلى عدة أنواع رئيسية وذلك كما يلي:

- شبكات Vehicle Ad Hoc Network (VANET)
- شبكات Wireless Sensor Network (WSN)
- شبكات Mobile Wireless Ad Hoc Network (MANET)
- شبكات Wireless Body Sensor Network (WBSN)

2-1 شبكات Vehicle Ad Hoc Network (VANETs):

تعتبر شبكة VANET أحد أهم أنواع الشبكات النقّالة الخاصة "Ad hoc" حيث أن العقد في هذا النوع من الشبكات عبارة عن عربات تؤلف شبكة فيما بينها وبين نقاط ثابته على الطريق لتبادل المعلومات، والهدف من هذه الشبكات هو توفير الأمان عن طريق تزويد السائقين بمعلومات عن الطريق، بالإضافة إلى تقديم خدمات للتسلية بالاعتماد على العديد من نمازج محاكاة حركة العربات وفق عدة نماذج تنقل، والتي تحدد الحركة لهذه العربات على الطرق بشكل أقرب ما يكون الى الواقع [12].

تعتبر بروتوكولات التوجيه أهم ما يميز أداء هذه الشبكات بسبب طبيعتها المتغيرة وبسبب تطور صناعة المركبات يوماً بعد يوم، اذ يتم ادخال التقنيات الجديدة المتمثلة بالعقول الإلكترونية وأجهزة الاتصالات الذكية لجعل استخدام الطريق أكثر راحة وأمان.



الشكل(2-1) شبكة VANET

في هذه التقنية كل مركبة تكون مزوده بجهاز اتصال لاسلكي لتتمكن المركبات من التواصل فيما بينها بالإضافة الى أبراج تتوضع على جانبي الطريق لربط المركبات البعيدة بعضها ببعض أو لتقديم خدمات إضافية مثل الانترنت وحتى ربط القطارات والطائرات بهذه الشـــبكات مما يجعل حجم تبادل المعلومات كبيراً جداً، وتســـمح هذه الشـــبكات بتبادل رسائل السلامة والطوارئ بين السائقين فعند حدوث حادث سير ترسل إحدى العربات المتسببة بالحادث أو القريبة منه برساله لكل المركبات المتوجهة لمكان الحادث لتبليغهم بمكان الحادث وبعض المعلومات عن حالة الطريق أمامهم.

2-1-1 المميزات الأساسية لشبكات VANETs عن بقية أنواع شبكات Ad Hoc:

- تتحرك العقد ضمن مسارات محددة هي الطرقات.
- تغيرات سريعة في طوبولوجيا الشبكة.
- لا توجد قيود على الطاقة أو تخزين البيانات.
- تستطيع العقد تحديد مواقعها عن طريق GPS.
- لا يوجد قيود على عرض الحزمة حيث أن الرسائل المتبادلة تكون ذات حجم صغير.
- نموذج تنقل العقد يُحدَد بمجموعة من العوامل مثل الإشارات الضوئية وحدود السرعة وحالة الحركة المرورية وسلوك السائقين.

2-1-2 مكونات شبكة VANETs:

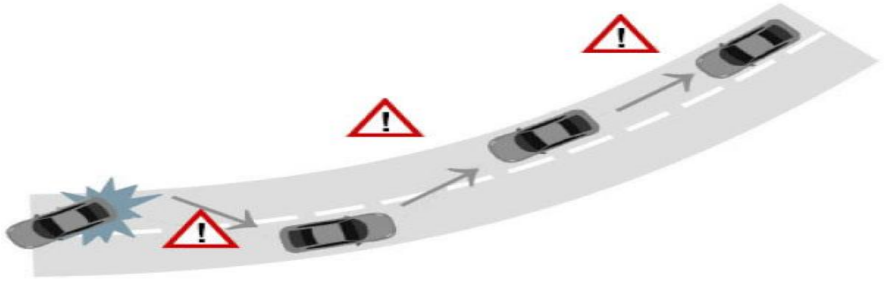
تتكون شبكة VANET من الأجزاء التقسيمات التالية:

1. **مجال العربة المتنقلة (In-Vehicle Domain)**: وتتكون من وحدتين هما:

- وحدة الاتصال ((On-Board Unit (OBU)): مسؤولة عن تحقيق الاتصال مع العقد الأخرى.
- وحدة التطبيق ((Application Unit (AU)): تمثل مجموعة من الحساسات لقياس الحالة الخاصة للعربة مثلا"(كمية الوقود)، ومعلومات بيئة القيادة مثلاً (المسافة الآمنة ومعلومات عن طريق غير معروف) ويمكن تبادل معلومات هذه الحساسات مع العربات الأخرى من أجل زيادة إدراك السائقين ببيئة القيادة لتحقيق ما يُسمى "أمن الطريق".

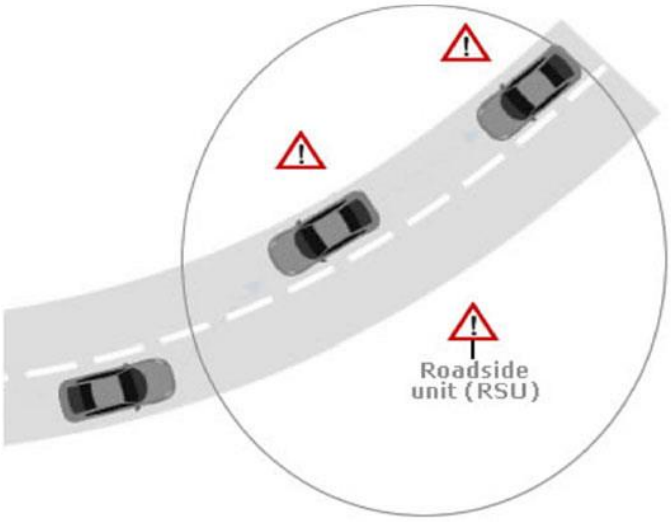
2. **مجال الشبكة (Ad Hoc Domain)**: ويتكون من:

- الاتصال عربة إلى عربة (OBUs to OBUs): وتُكتَب اختصاراً V2V أي Vehicles to Vehicles كما يلي:



الشكل (2-2) الاتصال V2V

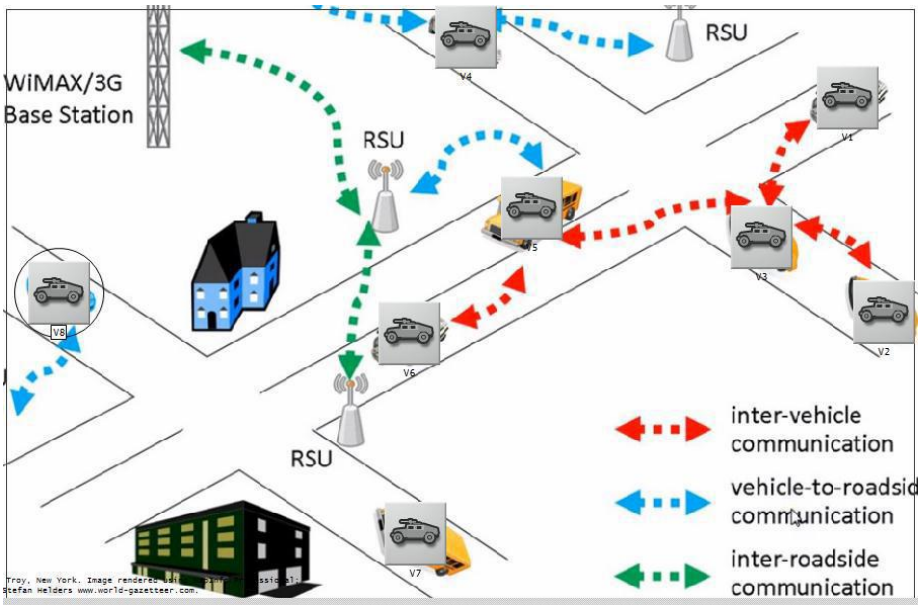
- الاتصال عربة الى بنية تحتية (Vehicles to Infrastructure (OBUs to RSUs)): وتُكتَب اختصاراً V2I كما يلي:



الشكل (2-3) الاتصال V2I

3. **مجال البنية التحتية (Infrastructure Domain)**: ويتضمن ما يلي:

- اتصال بين وحدات ثابتة على جانب الطريق (Road Side Unit) أي RSUs to RSUs.
- تقديم خدمات مثل الوصول إلى الانترنت (RSUs to Internet)، وتعد كبوابة عبور بين البنية التحتية والعربات.
- ويمكن أن تستخدم العربات أيضا" شبكات الخليوي (3G/4G) و Wi-Fi كما هو مُوضَح بالشكل التالي:



الشكل(2-4) أشكال الاتصال في شبكة VANET

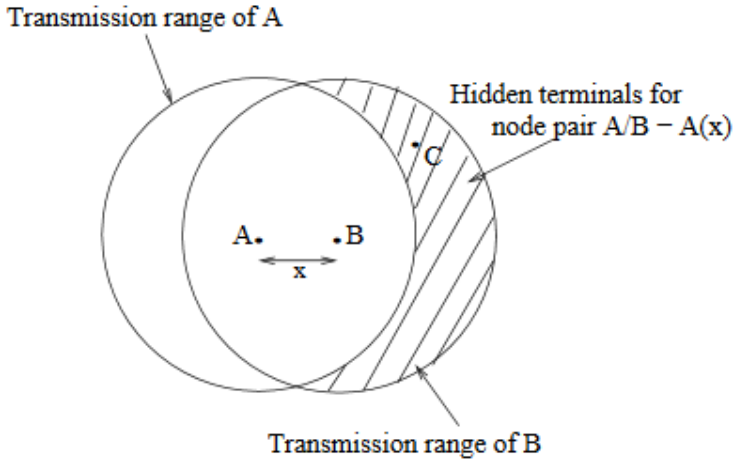
2-1-3 مشاكل الاتصال في شبكات VANETs:

توجد عدة مشاكل تعيق الاتصال في شبكات Ad hoc بشكل عام وشبكات VANET بشكل خاص وتتلخص هذه المشاكل في ثلاثة أنماط أساسية وهي:

1. مشكلة تصادم الإرسال (Transmission collision problem): تنشأ هذه المشكلة عندما تريد عقدتان من عقد الشبكة الاتصال مع عقدة أخرى وفي نفس الوقت، وهذا ما يسبب حدوث تصادم الإرسال القادم من مصدرين مختلفين وذلك عند العقدة المستقبلة بسبب وسط الاتصال المشترك، ويوضح الشكل التالي آلية حدوث التصادم:

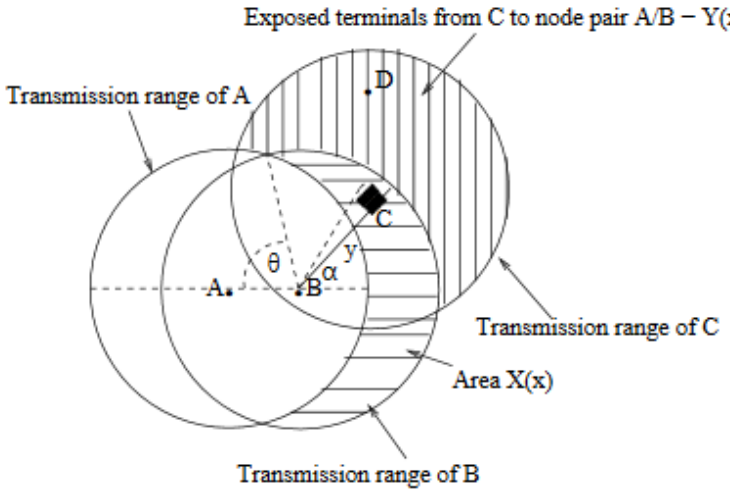
الشكل(2-5) مشكلة تصادم الإرسال

2. مشكلة الطرفية المخفية (Hidden terminal problem): تحدث هذه المشكلة عندما تريد عقدتان إرسال بيانات معاً في نفس الوقت إلى عقدة ثالثه، حيث تكون كل عقدة من العقدتين المرسلتين مخفية بالنسبة للعقدة الأخرى (خارج مجال تغطيتها)، لكن العقدة المستقبلة تكون ضمن مجال تغطية كل من العقدتين المرسلتين، فيحصل تصادم عندها ويتم اسقاط البيانات [13].



الشكل(2-6) مشكلة الطرفية المخفية

3. مشكلة الطرفية الظاهرة (Exposed terminal problem): تحدث هذه المشكلة أثناء محاولة منع التصادم حيث إن كل عقدة مرسلة تقوم بتفحص وسط الإرسال المشترك قبل البدء بعملية إرسال البيانات، فإذا وُجِدَت عقدتين كل منهما تقع ضمن مجال تغطية العقدة الأخرى، وكل منهما تريد إرسال البيانات في نفس الوقت لكن لوجهتين مختلفتين، في هذه الحالة سوف تدخل إحدى العقدتين المرسلتين في فترة انتظار غير مبررة بهدف منع التصادم الذي لن يحصل ابداً [13].



الشكل(2-7) مشكلة الطرفية الظاهرة

2-1-4 تصنيف بروتوكولات التوجية في شبكة VANETs:

2-1-4-1 البروتوكولات المعتمدة على الطوبولوجيا (Topology-based routing): يعتمد هذا النوع من البروتوكولات في اختيار المسار من المنبع إلى الهدف على المعلومات التي جُمِعت من قبل العربة المتنقلة بشكل مُسبَق(proactive/table-driven) أو عند الحاجة (reactive/on-demand) [14].

2-1-4-2 البروتوكولات المعتمدة على الموقع (Position-based routing): تستخدم المعلومات الجغرافية للعربات إذ تفترض أن كل عربة تمتلك وسيلة لمعرفة مواقعها الجغرافي مثل تقنية GPS، وفي هذا النوع من البروتوكولات ليس من الضروري معرفة المسار كاملاً من المصدر للهدف [14].

2-1-4-3 البروتوكولات المعتمدة على العناقيد (cluster-based routing): يمكن أن تشكل العربات التي تتشارك في الخصائص مثل الحركة في نفس الاتجاه وبسرعة أقل أو أكثر من السرعة نفسها عنقوداً بحيث يتم اختيار إحدى العقد لتكون قائد لهذه العنقود، وتكون مهمته إدارة الاتصالات بين العناقيد، في حين تتم الاتصالات داخل العنقود بين العقد دون تدخل قائد العنقود وباستخدام وصلات مباشرة.

2-1-4-4 بروتوكولات (Geocast-based routing): وهي برتوكولات متعددة البث معتمدة على الموقع، فهي تقدم خدمة ضمن منطقة جغرافية محددة، وهدفها إيصال الرزم من عقدة ما إلى كل العقد الموجودة ضمن منطقة جغرافية محددة تُدعى المنطقة ذات الصلة (ZOR(Zone of relevance، حيث أن العقد الموجودة خارج منطقة ZOR لا تصلها أي رسالة، وتهدف هذه البرتوكولات إلى تخفض الحمل الزائد والازدحام ضمن الشبكة والذي ينتج عن الغمر التقليدي للرزم في كل مكان ضمن الشبكة، وتعاني هذه البروتوكولات من مشكلة التقسيم غير المناسب للشبكة مما يعيق عملية التوجيه الصحيح للرسائل.

2-1-4-5 البروتوكولات المعتمدة على البث العام (Broadcast-based routing): تتميز بما يلي:

- تستخدم غالباً من أجل تطبيقات مثل حالة الطقس، حالة الطريق، حالات الطواريْ...
- تعتمد على إيصال الرزم إلى كل العقد ضمن الشبكة (غمر).
- مشكلتها الأساسية هي ضياع في عرض الحزمة والاستقبال المكرر للرزم من قبل العقد.

2-1-4-6 البروتوكولات المعتمدة على البنية التحتية (Infrastructure-based routing): تعتمد هذه البروتوكولات في عملها على عقد البنية التحتية مثل الوحدات الموجودة على جانبي الطريق (RSU).

2-2 شبكات الحساسات اللاسلكية WSNs:

ظل اتصال الحاسوب بأجهزة القياس أو أجهزة التحكم لوقت زمني طويل مقتصراً على الاتصال السلكي المباشر بين الحاسوب من جهة وتلك الأجهزة من جهة أخرى، وهذا الاتصال السلكي قد وضع – ولا شك – قيوداً على التطبيقات التي يمكن أن يقدمها الحاسوب في هذا المجال، ومن ناحية أخرى أتاحت التطورات العلمية المستمرة في السنوات الأخيرة في مجالي الإلكترونيات والاتصالات اللاسلكية تصنيع حساسات لاسلكية تعمل بالبطارية، وتتميز بصغر الحجم، وانخفاض التكلفة، وتعدد الاستخدامات، كما أنه يمكنها الإرسال لاسلكياً لمسافات مختلفة، وسمح تصنيع تلك الحساسات اللاسلكية بوجود تقنية جديدة تُسمى شبكات الحساسات اللاسلكية (Wireless Sensor Network) واختصاراً (WSN)، لتصنع الأخيرة بدورها جسراً بين عالم تكنولوجيا المعلومات والطبيعة التي نحيا فيها [15].

2-2-1 عقدة الحساس في شبكات WSNs:

تتكون من خمس وحدات أساسية يلزم وجودها في كل عقدة من عقد الحساسات اللاسلكية، وهناك بعض الأجزاء الإضافية التي قد توجد في العقدة وفق الحاجة إليها، وهذه الوحدات هي:

1. **الذاكرة:** وتُقسَم إلى قسمين:
   - ذاكرة لتخزين البرامج: يتم فيها تخزين التعليمات ليتم تنفيذها فيما بعد بواسطة المعالج.
   - ذاكرة البيانات: يتم تخزين المعلومات المحسوسة كدرجة الحرارة المقاسة وغيرها.

2. **المعالج:** يقوم بمعالجة المعلومات التي قامت العقدة بنفسها بجمعها أو التي وصلت إليه من العقد الأخرى.

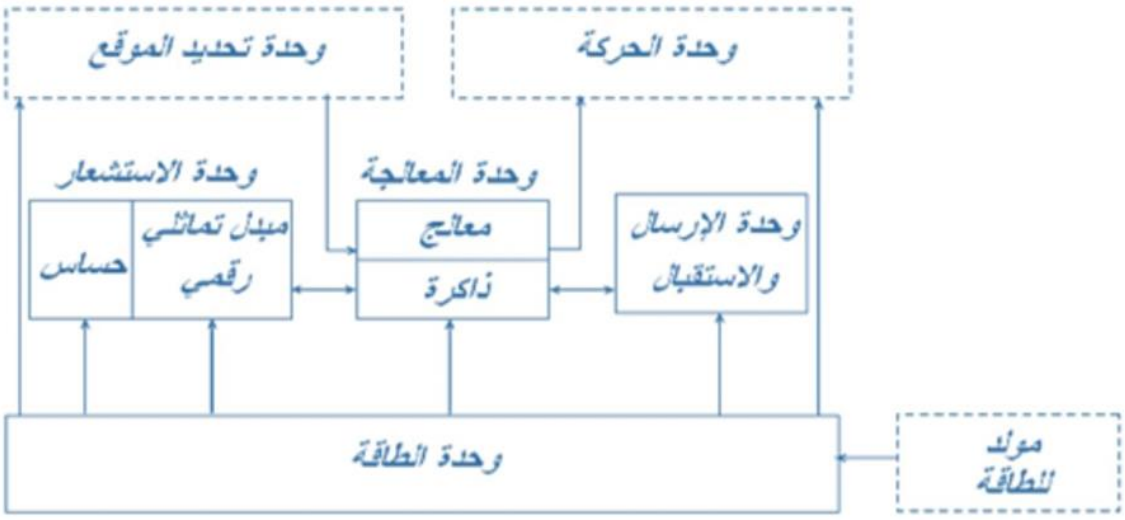
3. **الحساس:** يتخلف نوع الحساس باختلاف الهدف المراد من الشبكة نفسها، وقد تحتوي العقدة الواحدة على عدة حساسات منها تقيس الحرارة، وغيرها للضغط أو الرطوبة أو الضوء أو التسرب النفطي وغيرها للاهتزازات.

4. **مصدر الطاقة:**
   - البطاريات: وهي الأكثر استخداماً حيث تعطي الشبكة مرونة في توزيع عقدها الحساسة على البيئات المختلفة، وعادة ما تكون هذه العقد مزودة ببطاريتين AA قابلتين للشحن.

- الخلايا الشمسية: تُستخدم عندما لا تشكل التكلفة المادية موضوع حرجاً لتنفيذ التطبيق، أو في البيئات التي تتميز بمعدل جيد من الأيام المشمسة.

5. **وحدة الإرسال والاستقبال:** تُسمى وحدة البث حيث تكون كل عقدة مُجهزة بوحدة إرسال واستقبال تمكنها من الاتصال مع باقي العقد، ويكون النطاق القادرة على تغطيته أصغر من 100 متر، وتوجد حالياً حساسات بمجالات تغطية أكبر، فهي أكثر الوحدات استهلاكاً للطاقة، فهي تأخذ حوالي 97% من طاقة العقدة.
6. **وحدات إضافية:** تختلف هذه الوحدات حسب نوع التطبيق المُستخَدم وهي:

- **وحدة الحركة:** تستخدم في التطبيقات التي تحتاج إلى تحريك الحساسات من أماكنها.
- **GPS:** لتحديد موقع العقدة بدقة من حيث خط الطول والعرض والارتفاع.
- **وحدة خدمة الحزمة العامة الراديوية (General Packet Radio Service unit).**



الشكل(2-8) مكونات عقدة الحساس

2-2-2 طرق نشر العقد في شبكات WSNs:

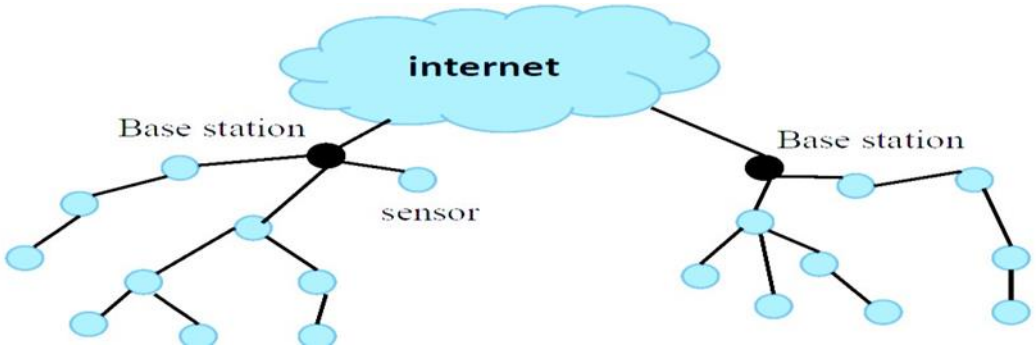
عادة ما تنتشر عقد الحساسات اللاسلكية في منطقة محددة، وهو ما يُطلق عليه اسم حقل الاستشعار، مكونة بذلك شبكة من الحساسات اللاسلكية (Sensor Filed)، وتوضع العقد اللاسلكية في الشبكة قد يكون بصورة منتظمة أو عشوائية، وذلك تبعاً لطبيعة البيئة المحيطة وطبيعة التطبيق المستخدمة فيه كما يلي:

- التموضع بصورة منتظمة: مثال على ذلك: ترتيب العقد لعمل شبكة لاكتشاف الحرائق في مبنى معين.

- التموضع بصورة عشوائية: مثال على ذلك: شبكة مماثلة لاكتشاف الحرائق في منطقة الغابات، حيث يتم توزيع العقد عن طرق طائرة.

ويكون لدى كل عقدة من العقد المنتشرة في الشبكة القدرة على استشعار البيئة المحيطة، ومن ثم جمع البيانات المطلوبة، ثم تُرسِل هذه العقد البيانات إلى المحطة الرئيسية والتي يستطيع المستخدم من خلالها أن يتعامل مع البيانات التي جُمِعت، وتتم عملية توجيه البيانات من عقد الحساسات اللاسلكية إلى المحطة الرئيسية أو المحطات الرئيسية ي حال تعددها في صورة قفزات متعددة (multi hops) من عقدة إلى أخرى باتجاه المحطة الرئيسية، ويكون مدى الإرسال لكل عقدة محدودا من أجل الحفاظ على الطاقة الموجودة لكل عقدة لأن الطاقة المستهلكة في إرسال البيانات تتناسب طردا مع مربع مدى الإرسال [16].

فنقول إن شبكة Ad hoc هنا هي مجموعة من العقد التي تتصل مع بعضها البعض لاسلكياً، وتكون هذه الشبكة لامركزية ولا تعتمد على بنية تحتية موجودة سلفاً لبناء طوبولوجيا الشبكة عليها، بحيث تتكون من عدد كبير من التجهيزان صغيرة الحجم ذاتية التغذية قادرة على جمع المعلومات من الوسط المحيط بها مثل درجة الحرارة والرطوبة والاهتزاز، وبشكل مستقل ومن ثم إرسالها لاسلكياً إلى مركز للمعالجة أو اتخاذ القرار أو محطة المراقبة، كمثال عليها شبكات حساسات لاسلكية تُستخدَم لمراقبة منطقتين جغرافيتين مختلفتين وتتصل بالإنترنت باستخدام محطات قاعدية قد يكون إما بهدف التخزين أو المعالجة أو التحليل كما يلي:



الشكل(2-9) شبكة ad hoc متصلة بالإنترنت

2-2-3 التحديات والقيود والخصائص في شبكات WSNs:

1. **الوسط الناقل للبيانات:** وهو عبارة عن وسط لاسلكي وهنا تظهر مشكلة التداخل بين مجالات التغطية للعقد المختلفة، الأمر الذي يجب أخذه بالحسبان ومحاولة تخفيضه قدر الإمكان من خلال نشر فعّال للعقد.
2. **الوسط المحيط:** تعمل عقد الحساسات اللاسلكية في أماكن مختلفة وظروف متنوعة تبعاً للتطبيق الذي تُستخدَم فيه، فتتنوع الظروف والأماكن بين وضع العقد بالقرب من الآلات في المصانع وداخل الأبنية والمنشآت، أو على سطح المياه في البحار والمحيطات، أو تثبيتها في جدران برية وبحرية، أو في مناطق مُعرضة لهجوم كيميائي أو نووي، وهذا ما يعني وجوب وضع الظروف المحيطة بالعقد في الحسبان عند صناعة تلك العقد.
3. **الكثافة:** تتميز أغلبية تطبيقات الحساسات اللاسلكية باعتمادها على شبكات فيها عدد كبير من العقد الأمر الذي يجعل عملية التحكم فيها وإدارتها وحتى مراقبتها أمراً صعباً، وكثير من التطبيقات تتطلب سرعة في نشر العقد وهذا بدوره يتطلب سرعة تشغيل هذه العقد، وكذلك القدرة على صيانتها بسهولة، فيتم ذلك عن طريق تطوير برمجيات خاصة بعقد الحساسات لتسمح بسرعة تشغيل بعد تكوين الشبكة.
4. **محدودية المصادر للعقد:**
   - محدودية الذاكرة
   - محدودية قدرة المعالجة
   - محدودية مجال الاتصال
   - محدودية الطاقة.
5. **القدرة على التنظيم الذاتي:** تتمتع العقدة الحساسة بقدرتها على التعرف على العقد الجارة لها، وأن تبدأ عمليات الإرسال والاستقبال بما يخدم التطبيق دون الحاجة إلى إدارة مركزية تقوم بتوجيه التطبيق كاملاً.
6. **التطبيقات المتنوعة:** عسكرية وطبية وصناعية وتجارية وكذلك تدخل مجال الزراعة والري، فإن وجود أصناف متنوعة من الحساسات يفسح المجال أمام ظهور تطبيقات كثيرة لشبكات الحساسات اللاسلكية.

إذ يوجد حساسات الرطوبة، وأخرى للحرارة، وحساسات قادرة على كشف التسريب النفطي، وأخرى تقيس الاهتزازات الأرضية، إضافة لإمكانية استخدام حساسات متحركة وثابتة.

7. **التكلفة المادية:** تتميز عقدة الحساس بتكلفة مادية منخفضة شجعت على استخدامها الواسع.

2-2-4 أنواع شبكات WSNs:

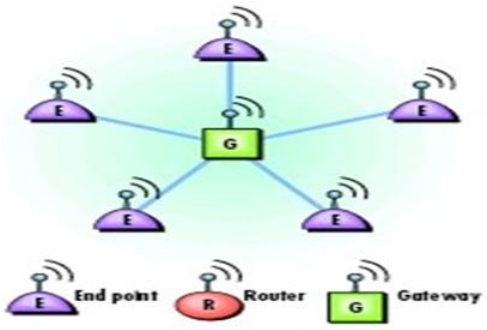
يوجد عدة أنواع لشبكات الحساسات اللاسلكية وذلك وفق التصنيفات التالية:

1. **البنية:** وتُقسَم إلى:

- **الشبكات المتجانسة:** تتكون من عقد متماثلة من حيث المواصفات مثل حجم الذاكرة، مجال الاتصال، الطاقة وغيرها.
- **الشبكات الهجينة:** تتكون من نوعين أو أكثر من العقد المختلفة من حيث المواصفات، أي تتفاوت من حيث مجال الاتصال وحجم الذاكرة وقدرة المعالجة.

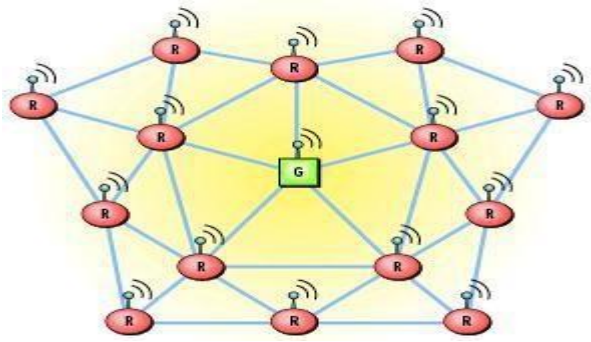
2. **الطوبولوجيا: وتُصنَف وفق الأنواع التالية:**

- الطوبولوجيا النجمية (star): كل العقد تتصل بشكل مباشر مع مركز المعالجة (sink)، كما يوضح الشكل التالي:



الشكل(2-10) الطوبولوجيا النجمية

- الطوبولوجيا متعددة القفزات (Mesh): العقد تتصل مع بعضها البعض مشكلةً مسارات للوصول إلى مركز المعالجة (sink)، كما يوضح الشكل التالي:



الشكل(2-11) الطوبولوجيا المتعددة القفزات

- الطوبولوجيا الهجينة: تتكون من النوعين السابقين معاً.

3. طريقة نشر العقد ضمن منطقة الاختبار:

- **نشر محدد:** مواقع العقد تكون محددة بشكل مسبق وتوضع بشكل يدوي.
- **نشر عشوائي:** مواقع العقد غير محدد وتتوزع بشكل عشوائي وذلك لأجل التطبيقات التي يصعب الوصول إلى منطقة الاختبار أو لأجل شبكة نوعاً ما حجمها كبير.

4. نموذج الحركة:

- **شبكة ثابتة:** تكون العقد والمركز ثابتة في مواقعها.
- **شبكة متحركة:** تكون إما العقد متحركة، أو المركز متحرك، أو كلاهما.

2-2-5 مقارنة بين شبكات WSNs وشبكات MANETs:

- **أوجه التشابه:**

1. كلاهما ليس لها بنية تحتية ثابتة ومحددة لأنها شبكات Ad hoc
2. عدم وجوب الإرسال بصورة مباشرة من عقد إلى اخرى: أي يمكن أن يتم الإرسال من خلال العقد التي بينها عن طريق قفزات متلاحقة من عقدة إلى أخرى وكذلك في كون الإرسال والاستقبال في كلتا الشبكتين لا سلكياً [17].

- **أوجه الاختلاف:**

1. **الأجهزة المستخدمة:** في شبكات الحواسيب الجوالة "MANET" هي Laptop أو PDA، أما في شبكات الحساسات اللاسلكية "WSN" فهي عقد الحساسات، حيث أن أجهزة الحواسيب المحمولة تمتلك إمكانيات أكبر بكثير من عقد الحساسات من حيث سرعة المعالج وقدرته، وحجم الذاكرة، وعمر البطارية.

2. **التطبيقات:** في MANET تعتمد التطبيقات في الأساس على نقل بيانات من جهاز محول إلى أخر وتوفير الخدمات بين الأجهزة المختلفة، بينما في WSN تعتمد التطبيقات على قياس بعض العوامل الطبيعية الموجودة في البيئة التي وُضِعَت فيها الشبكة وتسجيلها.

3. **التفاعل مع البيئة المحيطة:** تختلف WSN عن الشبكات عامة وعن شبكات MANET خاصة في كونها تتفاعل مع البيئة المحيطة من حيث قراءة معلومات نابعة من البيئة المحيطة مثل درجة الحرارة وغيرها وتسجيلها، وهذا يجعلها مختلفة عن الشبكات التقليدية التي يخضع نقل البيانات فيها للعامل البشري الذي يكون مسؤولا بصورة مباشرة أو غير مباشرة عن تبادل المعلومات ونقلها من حاسوب إلى أخر.

4. **معدل نقل البيانات:** في WSN عادة ما يكون منخفضاً وفي أوقات زمنية متباعدة، يحدث ذلك عندما تكون العوامل التي يتم قياسها مستقرة أو تتغير بصورة بطيئة، وينعكس الوضع في شبكات الحساسات اللاسلكية عندما يحدث أمر طارئ في البيئة المحيطة فيصبح التغير سريعاً، ويرتفع معدل نقل المعلومات بصورة كبيرة وهذه التغيرات عادة ما تحدث بصورة مفاجئة لا يمكن توقعها مسبقاً، مثلما يحدث عند نشوب حريق، في حين يكون معدل إرسال البيانات في شبكات الحاسبات الجوالة منتظماً، أو على الأقل يتبع نمطاً محدداً يمكن استنباطه بصورة مسبقة، ومن ثم يمكن تنظيم الإرسال على أساس ذلك.

5. **الطاقة:** أصبح معدل استهلاك الطاقة هو أحد أهم المقاييس في الحكم على كفاءة شبكات الحساسات اللاسلكية، وكثيراً ما تكون البطارية المستخدمة في العقدة غير قابلة للشحن، ومن ثم فإن الحاجة تكون ماسّة لإطالة عمر عقدة الحساسات اللاسلكية إذ يؤثر تأثيرا عميقا في بنية WSN، في المقابل تعمل البطاريات

في أجهزة الحواسيب المستخدمة فيMANET لمدة زمنية أطول وتكون ذات طاقة كهربائية أعلى، وعادةً ما يكون إعادة شحنها بسهولة عند توافر مصدر كهربائي.

6. تغير شكل الشبكة: في شبكات WSN يتغير وضع الشبكة تبعاً لفقد عقد الحساسات اللاسلكية نتيجةً لنفاذ الطاقة، بينما في شبكات MANET يتغير وضع الشبكة وفق حركة أجهزة الحاسوب.

2-3 شبكات Wireless Body Sensor Network (WBSNs):

إن شبكات حساسات الجسم اللاسلكية (WBSNs) هي إحدى تطبيقات شبكات الحساسات اللاسلكية، حيث أن وظيفتها الأساسية هي قياس وجمع المعلومات الحيوية الخاصة بجسم الكائن الحي [18].

تتألف WBSNs من عقد حساسات ذكية لا تعيق أنشطة الحياة اليومية للإنسان، وهي مفيدة في الكشف عن الأمراض المزمنة مثل النويات القلبية والربو والسكري وغيرها ولتحذير المرضى في حالة الظروف الطارئة، باستخدام شبكات WBSNs يمكن رصد الأنشطة والحركات وإشارات الجسم الحيوية للإنسان من مكان بعيد باستخدام الإنترنت وهذا يساعد في توفير المال، ويتم تقسيم عقدها حسب تموضعها إلى:

- حساسات يتم ارتداؤها حول جسم الإنسان.
- حساسات يتم تثبيتها على جسم الإنسان.
- حساسات يتم توزيعها ضمن جسم الإنسان.

الشكل(2-12) أنماط تموضع العقد في شبكات WBSNs

2-3-1 الفرق بين شبكات WSNs وشبكات WBSNs:

بما أن شبكات WBSNs هي تطبيق من شبكات WSNs فهي تمتلك خصائص تشبه بعض خصائص شبكات WSNs ولكن تختلف عنها بعدة نقاط:

- **منطقة النشر:** تنتشر عقد شبكات WSNs في أغلب التطبيقات في مناطق لا يمكن الوصول إليها، بينما تقوم كل مجموعة من عقد WBSNs بمراقبة العلامات الحيوية لكائن بشري.
- **كثافة النشر:** تنتشر عقد WSNs بشكل كثيف من أجل ضمان عدم خروج الشبكة عن العمل في حال تعطل عدد من العقد، لكن في شبكات WBSNs يكون لكل جسم عدد محدد من العقد، ولكل عقدة وظيفة مختلفة.

- **حجم العقدة:** لا يشكل حجم عقدة الحساس دوراً مهماً في شبكات WSNs، ولكن حجم العقدة أمر مهم وحرج جداً في عقد WBSNs، وذلك من أجل ضمان حرية حركة الإنسان وعدم تأثيرها على حياته اليومية.

- **مصدر الطاقة:** إن مصدر الطاقة في عقد WSNs هي إما البطاريات أو الطاقة الشمسية أو قد تكون الطاقة المولدة من طاقة الرياح، بينما يتم تغذية العقد في WBSNs عن طريق الطاقة الحرارية والحركية للجسم.

- **معدلات الإرسال:** معدلات الإرسال في عقد WSNs تكون متساوية، بينما في عقد WBSNs تختلف من عقدة لأخرى بحسب البيانات المسؤولة عن تحسسها وجمعها، وبحسب موقع العقدة.

2-3-2 بنية شبكات WBSNs:

تتألف بنية الاتصالات في WBSNs من ثلاث طبقات:

الطبقة الأولى (Intra BAN Communication): تتمثل هذه الطبقة ضمن مجال تغطية متر مربع وتقسم إلى نوعين:

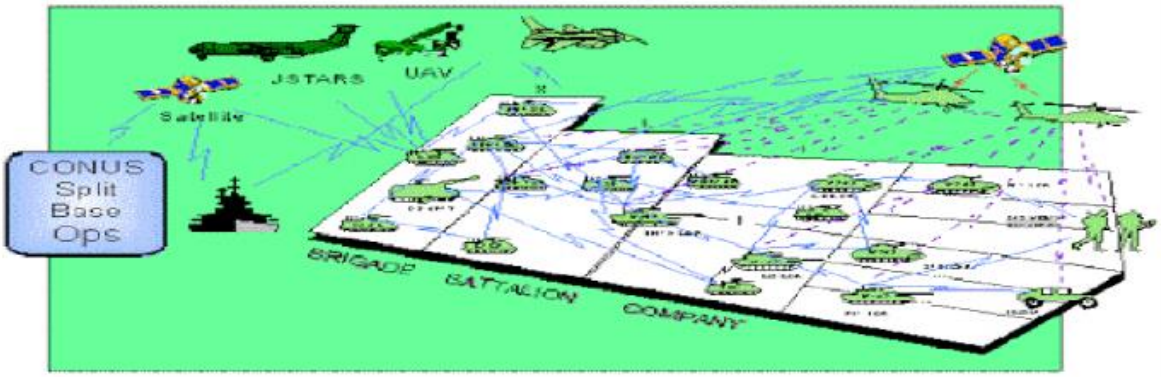
- الاتصالات بين عقد WBSNs ضن الجسم نفسه.
- الاتصالات بين عقد WBSNs ومركز المعالجة المحمول Sink

الطبقة الثانية (Inter BAN Communication): يتم ضمن هذه الطبقة اتصال مركز المعالجة المحمول (Sink) مع نقطة وصول (AP) واحدة أو أكثر.

الطبقة الثالثة (Beyond BAN Communication): تختلف مكونات هذه الطبقة باختلاف التطبيق المستخدم، فمثلا من أجل العناية بالصحة يتم الاتصال بين نقطة الوصول وقاعدة بيانات لتخزين جميع بيانات المريض، وبذلك تكون إمكانية الاطلاع عليها في أي وقت، كما يتم الاتصال بشكل مباشر إلى الطبيب المسؤول عن هذا المريض لمراقبة حالته الآتية وغيرها من بارامترات حيوية.

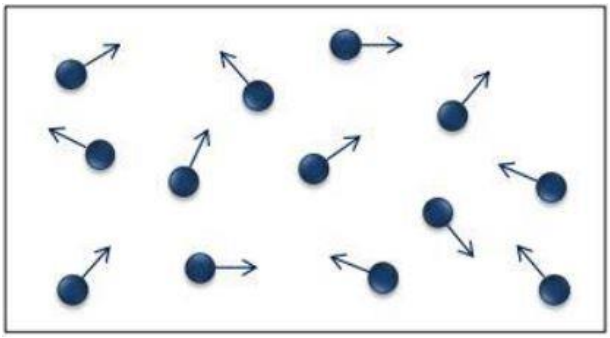
2-4 شبكات Mobile Wireless Ad Hoc Network (MANETs):

شبكات الحواسيب المحمولة (MANET) بالتعريف هي عبارة عن نظام ذاتي التنظيم self-governing حيث أنها تجميع لعقد لاسلكية متحركة بشكل ديناميكي مشكلة شبكة دون أي وجود لبنية تحتية أو تحكم مركزي، والغاية منها الوصول للمعلومات في أي مكان وأي زمان، حيث تتألف شبكة MANET من منصات متحركة (mobile platforms) حُرة الحركة عشوائياً، ويمكن اعتبارها نظام مستقل من العقد المُختارة حسب طبيعة ومكان الاستخدام، علماً أنه قد تتغير طوبولوجيا هذه الشبكة تبعاً لتغير مواقع العقد أو ضبط بارامترات الإرسال والاستقبال لها، وتُعتَبر الشبكات العسكرية أحد أهم تطبيقات شبكات الحواسيب المحمولة (MANET)، حيث أن هذا النوع من التطبيقات يسمح بتبادل المعلومات في بيئة لا توجد فيها بنية أو ذات البنية التحتية المدمرة، ويوضح الشكل (2-11) مثال لهذا النوع من الشبكات [19]:



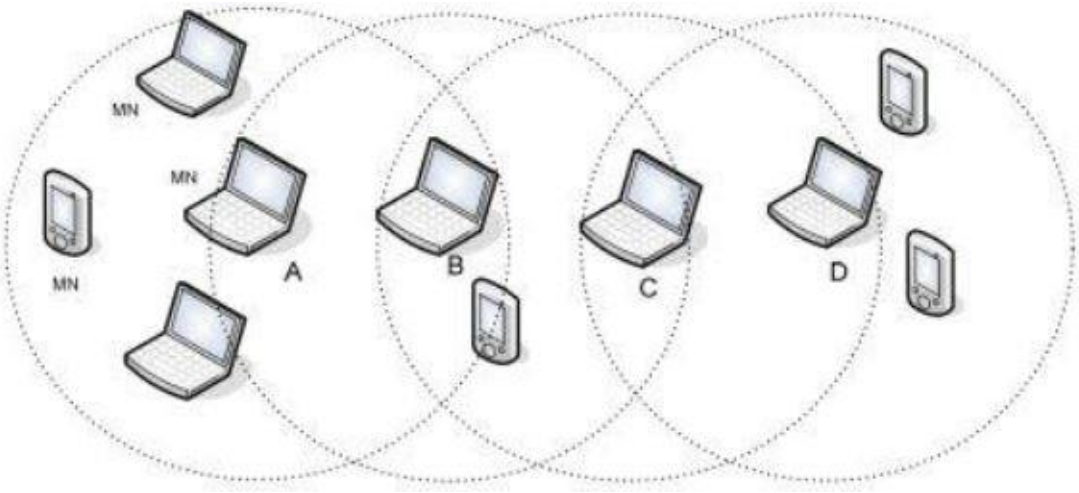
الشكل (2-13) شبكة MANET

في حالة شبكات MANETs تتغير طوبولوجيا الشبكة طوال الوقت بشكل سريع وغير متوقع نتيجة لحركة العقد، مما يجعل عملية توجيه الرسائل تحدياً حقيقياً في هذه الشبكات، يوضح الشكل (2-12) الحركة العشوائية والغير متوقعة للعقد في جميع الاتجاهات، وعلى الرغم من التحديات التي تواجهها شبكات MANETs في توجيه الرسائل، إلى أنها تتميز بسهولة وسرعة الإنشاء وبكلفة منخفضة بالمقارنة مع الشبكات التقليدية.



الشكل (2-14) الحركة العشوائية للعقد في شبكة MANET

يوضح الشكل (2-13) مثالاً لأحد سيناريوهات شبكة MANET، لنفترض أن العقدة A هي المصدر source node والعقدة D هي الهدف destination node، وأن كل منهما خارج مجال الإرسال للأخرى، وبالتالي لا يمكن للعقدة A إرسال البيانات بشكل مباشر للعقدة D، لذلك تتم عملية التوجيه routing بين العقدة A والعقدة B من خلال العقد الوسيطة B و C.



الشكل (2-15) مثال لأحد سيناريوهات شبكة MANET

2-4-1 الخصائص الأساسية لشبكات MANETs:

تتمتع شبكات الحواسيب النقالة MANETs (باعتبارها أحد أنواع الشبكات اللاسلكية) بالخصائص العامة للشبكات اللاسلكية، ولكن بعيداً عن هذه الخصائص العامة تمتلك أيضاً بعض الخصائص المميزة لها ونأتي فيما يلي على ذكر أهمها [20]:

2-4-1-1 الطوبولوجيا الديناميكية:

تعتبر الحركية mobility أحد أهم الخصائص لشبكات MANETs والتي تعطي للعقد أمكانية التحرك بكل الاتجاهات وبمختلف السرعات بدون انقطاع الاتصالات الفعالة طالما أن العقد لا تزال ضمن مدى الإرسال، حيث تتوضع العقد المتحركة بشكل حر وشجري، بالنتيجة فإن طوبولوجيا الشبكة يمكن أن تتغير بشكل لحظي سريع وعشوائي مما يسبب انقطاع المسار بين العقد المرسلة والعقد المستقبلة، علماً أن الوصلات يمكن أن تكون وحيدة الاتجاه أو ثنائية.

2-4-1-2 عرض الحزمة المحدود:

إحدى الخصائص الأساسية للشبكات المعتمدة على الاتصالات اللاسلكية هي استخدام وسط مشترك للاتصال، وإحدى نتائج هذا الوسط المشترك هو أن يكون عرض الحزمة المحجوز للمضيف متواضع.

2-4-1-3 قيود الطاقة:

يتم تغذية العقد في هذه الشبكات من مصدر طاقة مستقل مثل البطاريات، لذلك يجب أخذ بارامترات الطاقة بعين الاعتبار في كل الأمور المتعلقة بالتحكم في هذا النظام.

2-4-1-4 غياب البنية التحتية:

يتميز هذا النوع من الشبكات بغياب أي وجود لأي بنية تحتية، حيث لا يمكن لعقدة MANET أن تعتمد على وظائف دعم مركزي سواء للأغراض الأمنية أو التوجيه، وإنما يتم تصميم جميع وظائف الدعم لتعمل في عقدة MANET بشكل مستقل دون تلقي أي دعم مركزي، وبذلك تكون الأجهزة المتحركة مسؤولة عن بناء وحفظ اتصالية الشبكة بشكل مستمر، علماً أن هذه الطبيعة الموزعة لشبكات MANETs تكسبها متانة ضد حالات single point of failure الموجودة في البنى المركزية.

2-4-1-5 محدودية الأمن الفيزيائي:

تُعد هذه الشبكات مُهددة كثيراً بالهجمات مقارنة بالشبكات السلكية، وهو ما يُعلل بالقيود والمحددات الفيزيائية التي تتحكم بالمعطيات المتنقلة والتي يجب تخفيضها.

2-4-1-6 الاتصال متعدد القفزات Multi-hop:

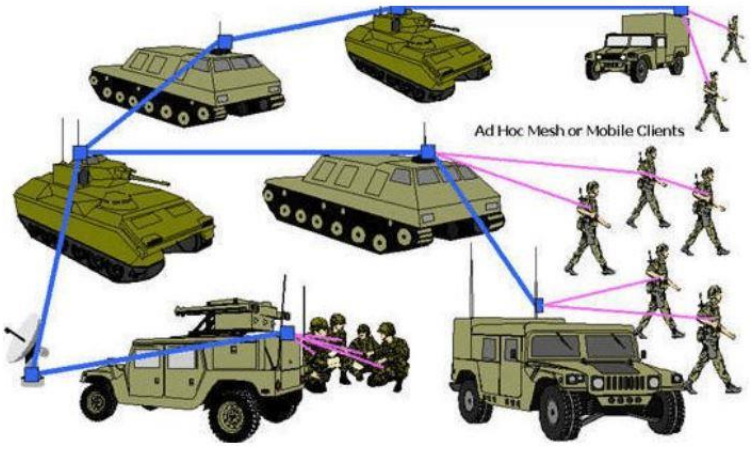
عندما تحتاج إحدى العقد في شبكة MANET لإرسال بيانات إلى عقدة أخرى خارج مجال الإرسال الخاص بها يتم إرسال هذه البيانات عبر العقد الوسيطة، حيث تُسمى هذه العملية بالاتصال متعدد القفزات multi-hop communication، إذاً وبمعنى آخر فإن كل عقدة في شبكة MANET قادرة على القيام بوظائف الموجة router لتوجيه طرود البيانات مما يساهم في تحقيق الوصلة متعددة القفزات، بالإضافة إلى امتلاكها إمكانيات المعالجة الأساسية لتعمل كمضيف host.

2-4-2 تطبيقات شبكات MANETs:

في البداية كانت تطبيقات شبكات MANETs ذات توجهات عسكرية، ولكن لاحقاً وبعد التقدم الكبير المتسارع بمجال شبكات MANETs بدأت التطبيقات الغير عسكرية بالظهور بشكل متزايد، حيث أصبحت هذه التكنولوجيات قابلة للتطبيق في العديد من السيناريوهات سواءً التعليمية أو التجارية أو عمليات البحث والإنقاذ، وحتى في الشبكات الشخصية Personal Area Networks (PAN) يوجد العديد من التطبيقات لتقنيات MANET ونقدم فيما يلي موجزاً لأهم هذه التطبيقات:

2-4-2-1 المجال العسكري:

عادة ما تكون التجهيزات العسكرية مزوده بوسائط اتصال لاسلكية، وبالتالي يمكن أن تساعد تكنولوجيا MANETs على مشاركة المعلومات في الميدان بين الجنود والعربات الحربية ومروحية القيادة، وكما ذكرنا سابقاً فأن التطبيقات الأولية لشبكات MANETs كانت عسكرية التوجه، لكن الأبحاث المتسارعة في هذا النوع من الشبكات ساعدت على ظهور تطبيقات غير عسكرية وتطورها بشكل سريع، وأحد الأمثلة على التطبيقات العسكرية يتضمن عمليات الاستطلاع لمعرفة مواقع العدو في الميدان.



الشكل (2-16) مثال للتطبيقات العسكرية لشبكات MANETs

2-4-2-2 المجال التجاري:

لقد كان العامل المحفّر للتطبيقات التجارية لشبكات MANETs هو الطبيعة عديمة البنية التحتية التي تتميز بها هذه الشبكات، مما يساعد على تجاوز الكلفة اللازمة للبنية التحتية، بالإضافة إلى توفر تجهيزات لاسلكية بتكلفة منخفضة، ونستعرض فيما يلي بعض الأمثلة للتطبيقات التجارية لشبكات MANETs:

- **الشبكات التشاركية Collaborative Networks:** تُستخدم الشبكات التشاركية في الحالات التي يرغب بها مجموعة من المستخدمين بمشاركة الملفات فيما بينهم دون استخدام شبكة الانترنت، على سبيل المثال لنفترض حالة قاعة مؤتمرات يتم فيها تبادل الملفات بين المشاركين، يمكن استخدام طيف واسع من التجهيزات لتبادل البيانات في مثل هذه الشبكات، مثل الحواسيب المحمولة أو الهواتف المحمولة أو غيرها من تجهيزات الاتصال.

- **الشبكات المنزلية Home Networks:** تتضمن الشبكات المنزلية الاتصال بين التجهيزات المنزلية الذكية وغيرها مثل الهواتف الذكية والحواسيب المحمولة، حيث إنه بما أن تقنيات MANETs تقلل من الحاجة لوجود عقد مركزية وتخفف من العبء الناجم عن الاتصال عبر هذه العقد، بالتالي فإن هذه التكنولوجيا ملائمة للاستخدام في تطبيقات الشبكات المنزلية.

2-4-2-3 حالات الطوارئ: تُعد شبكات MANETs اختياراً مناسباً للنشر في حالات الطوارئ وعمليات البحث والإنقاذ، فمثلاً في حالات الكوارث الطبيعية كالفيضانات أو الزلازل التي قد تؤدي إلى تدمير وسائل الاتصال، يمكن استعادة الاتصالات في المنطقة بسرعة عن طريق نشر شبكة MANET، حيث تتصل سيارات الإسعاف والإطفاء والشرطة مع بعضها مكونة شبكة MANET لتبادل المعلومات.

2-4-3 معايير الاتصال في شبكات MANETs:

يُعتبر المعهد الدولي لمهندسي الكهرباء والإلكترون IEEE المطور الأساسي للمعايير الدولية، وعلى وجه الخصوص تلك المتعلقة بالاتصالات وتقانة المعلومات وتوليد الطاقة الكهربائية، حيث يملك المعهد مجموعةً من 900 معياراً قيد الاستخدام و400 أخرى قيد التطوير [21].

من أكثر معايير IEEE شيوعاً هي مجموعة معايير IEEE 802 LAN/WAN، والتي تتضمن معيار شبكات الإيثرنت (IEEE 802.3) ومعيار الشبكات اللاسلكية (IEEE 802.11).

2-4-3-1 معيار الاتصال IEEE 802.11:

يمكن توصيف المعيار IEEE 802.11 ببساطة بأنه معيار شبكات الإيثرنت اللاسلكية وقد حدد هذا المعيار بروتوكول الوصول إلى الحامل بتحسس الناقل مع تجنب التصادم CSMA/CA كآلية للوصول إلى الحامل تماماً كما هو الحال في شبكات الإيثرنت، حيث تعتمد جميع تعديلات المعيار IEEE 802.11 على نفس آلية الوصول إلى أنّ فعالية بروتوكول CSMA/CA ضعيفة جداً نتيجة استهلاكه قسماً كبيراً من عرض الحزمة في سبيل ضمان موثوقية إرسال البيانات وتتواجد هذه المحدودية في جميع التقنيات المعتمدة على بروتوكول CSMA/CA.

يحدد المعيار IEEE 802.11 سرعتين أساسيتين لنقل البيانات وهما 1 و2 ميغا بت في الثانية للإرسال عبر الأشعة تحت الحمراء Infrared (IR) أو الأمواج الراديوية العاملة بتردد 2.4 غيغا هرتز على الرغم من عدم وجود أي تطبيق عملي حتى الآن للإرسال عبر الأشعة تحت الحمراء إلا أنها مازالت جزءً من المعيار الأصلي.

ظهرت في الأسواق عدة منتجات صممت وفقاً للمعيار IEEE 802.11 لكنها سرعان ما استبدلت بمنتجات متوافقة مع المعيار IEEE 802.11b بعد إقرار التعديل b على المعيار الأساسي.

يغطي المعيار IEEE 802.11 الطبقتين الأولى والثانية من النموذج المعياري OSI (Open Systems Interconnection) وهما الطبقة الفيزيائية Physical Layer وطبقة وصلة البيانات Data link Layer.

2-4-3-2 تعديلات المعيار IEEE 802.11:

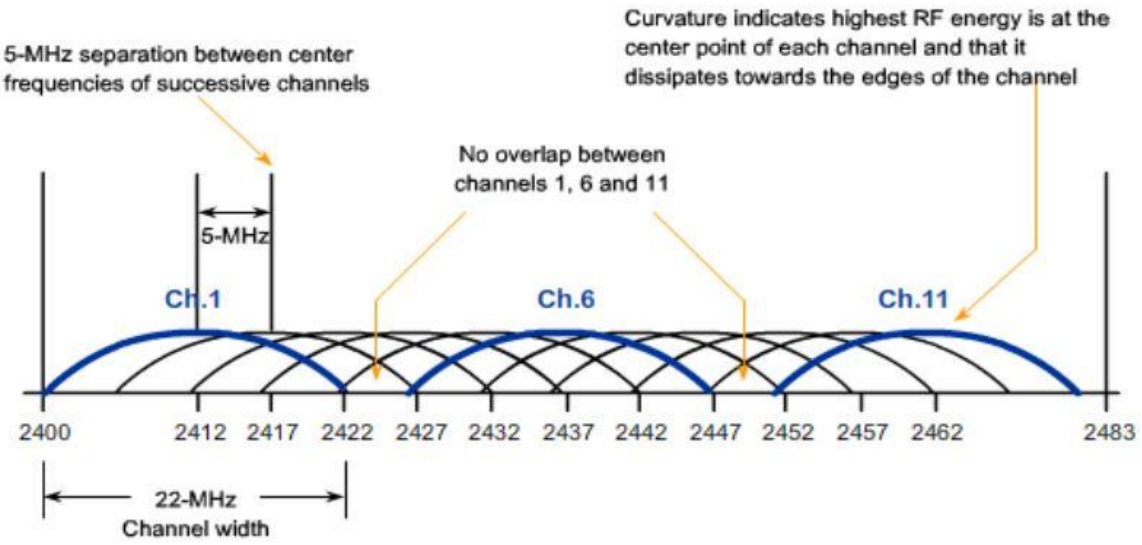
تعتبر التعديلات b،a و g والتي حققت انتشاراً واسعاً في السوق بفضل منتجات متوافقة ذات أسعار معقولة أكثر التعديلات شيوعاً ضمن عائلة معايير 802.11، ومن التعديلات الأخرى ضمن نفس العائلة هو المعيار n وهو عبارة عن تحسينات وتطويرات أو تصحيحات لمواصفات سابقة ضمن هذه العائلة، وسنلقي فيما يلي نظرة على التعديلات n، g، b،a .

معيار الاتصال IEEE 802.11b:

يتضمن المعيار IEEE 802.11b تحسينات على المعيار الأصلي 802.11 لدعم نقل البيانات بسرعات أكبر (5.5 و11 ميغا بت في الثانية)، يستخدم هذا المعيار نفس أسلوب الوصول إلى الناقل المحدد في المعيار الأصلي 802.11، ويستخدم أيضاً تقنية توزيع الطيف عبر التتابع المباشر المُحددة أيضاً في المعيار الأصلي 802.11.

يمكن لأي بطاقة للشبكة اللاسلكية متوافقة مع معيار 802.11 أن تنقل البيانات نظرياً بسرعة 11 ميغا بت في الثانية، إلا أنها سوف تقوم بتخفيض هذه السرعة وفق مقياس الاختيار المتكّيف لسرعة نقل البيانات إلى 5.5 ثم 2 ثم 1 ميغا بت في الثانية في حال حدوث أي ضياع في رزم البيانات.

تُعتبر السرعات الدنيا لنقل البيانات أقل حساسية للتشويش والتلاشي لأنها تستخدم اسلوباً أكثر موثوقية لترميز البيانات أي أن العلاقة بين الإشارة والضجيج تصبح أفضل في السرعات الدنيا.



الشكل (2-17) الحزمة الترددية 2.4 GHZ

معيار الاتصال IEEE 802.11a:

يستخدم هذا المعيار (تماماً كما هو الحال في المعيار IEEE 802.11b) نفس البروتوكول الأساسي المحدد في المعيار الأصلي، ويعمل المعيار IEEE 802.11a ضمن حزمة التردد 5 غيغا هرتز، ويستخدم تقنية ترميز تقسيم التردد المُتعامِد OFDM مما يعطيه القدرة على بلوغ سرعة قصوى لنقل البيانات تعادل 54 ميغا بت في الثانية، ويمكن تخفيض هذه السرعة باستخدام الاختيار المتكّيف لسرعة نقل البيانات إلى 48، 36، 24، 18، 12، 9 و6 ميغا بت في الثانية إذا ما اقتضت الحاجة.

لم يبلغ المعيار IEEE 802.11a حتى يومنا هذا الانتشار الواسع الذي حققه المعيار IEEE 802.11b، فمن معوقات استخدام هذا المعيار القوانين الأكثر صرامة في حزمة الترددات 5 غيغا هرتز.

معيار الاتصال IEEE 802.11g:

لقد تم استخدام التعديل الثالث للمعيار 802.11 في حزيران 2003 وأُعطي الاسم IEEE 802.11g، ويعمل هذا المعيار (شأنه شأن نظيرة IEEE 802.11b) ضمن الحزمة الترددية 2.4 غيغا هرتز، لكنه يستخدم نفس تقنية الترميز المعتمدة في المعيار IEEE 802.11a وهي OFDM مما يمكنه من بلوغ سرعة قصوى لنقل البيانات تصل حتى 54 ميغا بت في الثانية [22].

من أجل ضمان التوافقية مع المنتجات العاملة وفق معيار IEEE 802.11b فأن هذا المعيار يعود إلى استخدام تقنيات الترميز CCK+DSSS عند سرعات نقل البيانات 11 و5.5 ميغا بت في الثانية، في حين يستخدم ترميز DBPSK/DQPSK+DSSS عند سرعات 1 و2 ميغا بت في الثانية.

يعود الفضل في القبول الواسع الذي حظي فيه المعيار IEEE 802.11g بالدرجة الأولى إلى توافقيته مع التجهيزات العاملة وفق معيار 802.11b، علماً أنه يعاني من نفس مشاكل المعيار 802.11b فيما يتعلق بالتشويش في المواقع المزدحمة وذلك نتيجة استخدامه نفس حزمة الترددات.

802.11b / g			
رقم القناة	التردد المركزي (غيغاهرتز GHz)	رقم القناة	التردد المركزي (غيغاهرتز GHz)
1	2.412	8	2.447
2	2.417	9	2.452
3	2.422	10	2.457
4	2.427	11	2.462
5	2.432	12	2.467
6	2.437	13	2.472
7	2.442	14	2.484

الجدول (2-1) القنوات الترددية للمعيارين 802.11b/g

معيار الاتصال IEEE 802.11n:

يهدف هذا التعديل للوصول إلى سرعة نظرية قصوى لنقل البيانات تعادل 540 ميغا بت في الثانية، مما يجعله أسرع 40 مرة من المعيار IEEE 802.11b و10 من المعيار IEEE 802.11a، ويعتمد هذا المعيار على نفس التعديلات السابقة لمعيار 802.11 مع فارق أساسي يكمن في استخدام تقنية الدخل المتعدد–الخرج المتعدد (Multi Input–Multi Output MIMO) والتي تتطلب عدة مرسلات وعدة مستقبلات لزيادة سرعة نقل البيانات ونطاق الإرسال، ويوضح الجدول التالي مقارنة بين التعديلات الأكثر أهمية للمعيار **IEEE 802.11**.

المعيار	التردد	قيمة الترميز	سرعة نقل البيانات	ملاحظات
802.11a	5 GHZ	OFDM	54 Mbps	8 قنوات غير متداخلة، ولا يوجد جودة للخدمة
802.11b	2.4 GHZ	DSSS, CCK	11 Mbps	14 قناة متداخلة
802.11g	2.4 GHZ	OFDM, DSSS	54 Mbps	14 قناة متداخلة، متوافق مع معيار 802.11b
802.11n	2.4 GHZ	OFDM	540 Mbps	يعتمد على المعايير السابقة بالإضافة إلى تقنية MIMO

الجدول (2–2) مقارنة بين معايير الاتصال IEEE 802.11 a, b, g, n

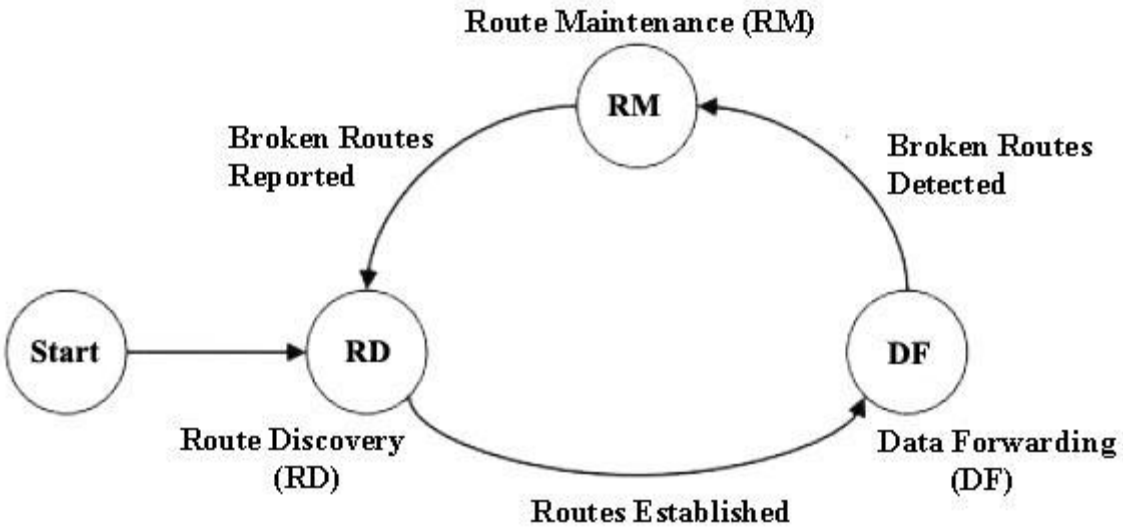
2–4–4 التوجيه في شبكات MANETs:

التوجيه routing في شبكة اتصال ما هو عملية اكتشاف المسار بين عقدة المصدر source node وعقدة الهدف destination node، تمثل عملية التوجيه في شبكات MANETs تحدياً كبيراً نتيجةً للخصائص المميزة لهذه الشبكات والتي سبق ذكرها، ونظراً لذلك فقد اهتمت العديد من الأبحاث بدراسة عملية إيجاد المسار الأمثل للاتصال بين العقدة المصدر والعقدة الهدف.

2-4-4-1 مراحل التوجيه في شبكات MANETs:

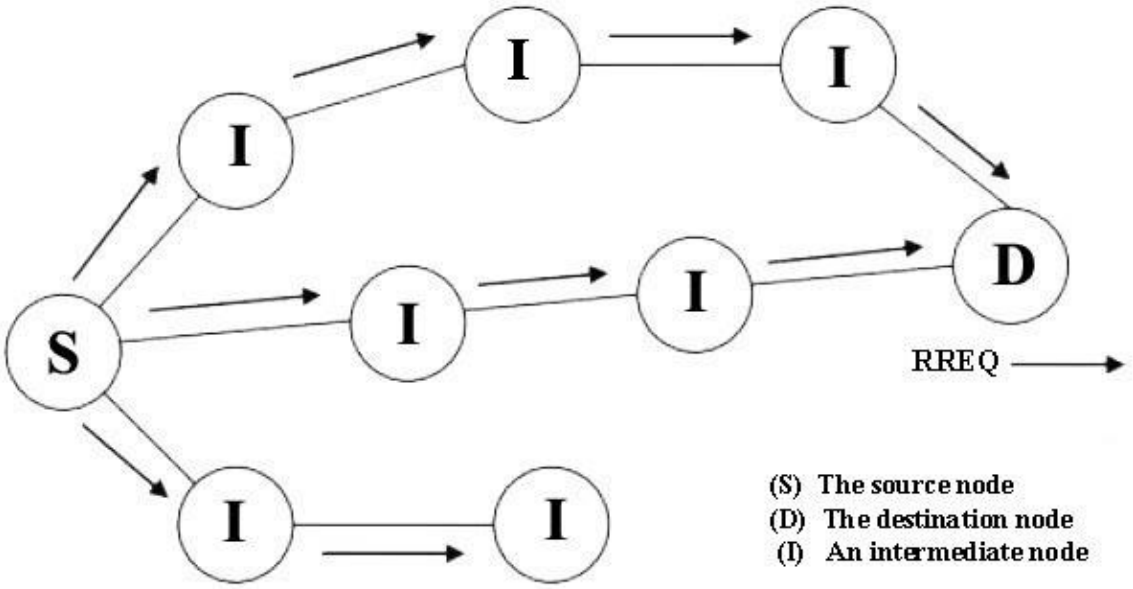
يمكن شرح عمليات التوجيه في شبكات MANETs وفق ثلاث مراحل كما يوضح الشكل (2-16) وهي مرحلة اكتشاف المسار Route Discovery ومرحلة إرسال البيانات Data Forwarding ومرحلة صيانة المسار Route Maintenance.

تبدأ عملية التوجيه بمرحلة اكتشاف المسار عندما تحتاج العقدة لإنشاء اتصال مع عقدة أخرى حيث تبدأ بالبحث عن مسار، ويبدأ الاتصال عندما يتم إيجاد مسار نحو الهدف وهنا تبدأ مرحلة إرسال البيانات Data Forwarding، وعندما يحصل انقطاع في احدى الوصلات أثناء إرسال البيانات نتيجة خطأ ما مثلاً نتيجة حركة العقدة أو نفاذ الطاقة، تبدأ عملية إيجاد مسار بديل يضمن استمرار الاتصال حيث تتعامل مرحلة صيانة المسار Route Maintenance مع حالات انقطاع الاتصال، ففي هذه المرحلة عندما تكتشف العقدة انقطاع الاتصال تحاول البحث عن مسار بديل في الذاكرة المحلية Local Cashe، وفي حال تعذر إيجاد مسار بديل في الذاكرة المحلية تبدأ العقدة مجدداً بمرحلة اكتشاف مسار جديد لنفس الوجهة.



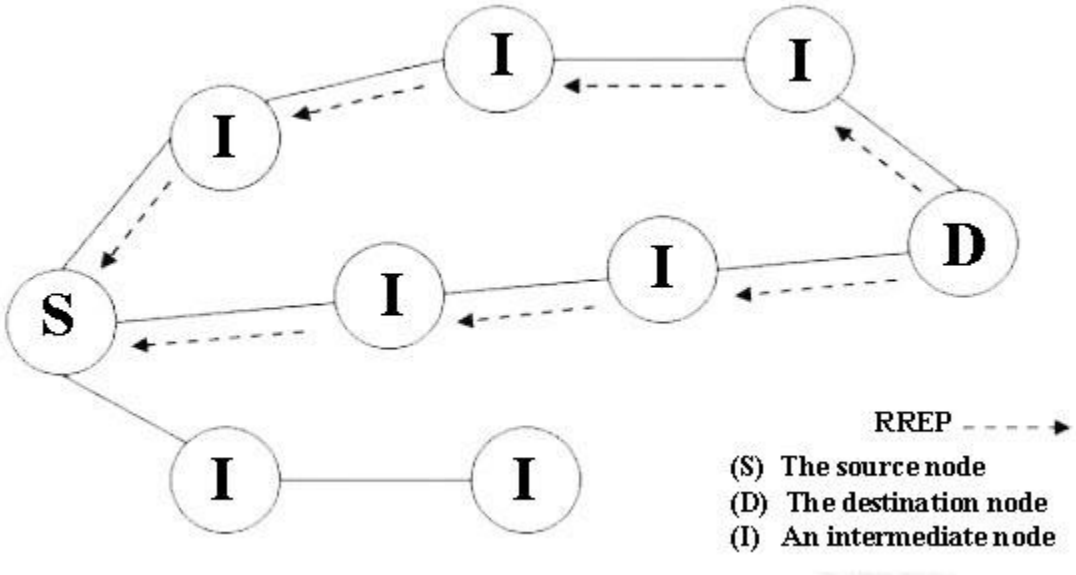
الشكل (2-18) مراحل عملية التوجيه في شبكات MANETs

كما ذكرنا فأن المرحلة الأولى في عملية التوجيه هي مرحلة اكتشاف المسار، وتنطلق هذه المرحلة عندما تنضم عقدة ما إلى الشبكة أو عندما ترغب احدى العقد source node بإنشاء اتصال إلى عقدة أخرى destination node، حيث تقوم عقدة المصدر بتفحص الجوار لإيجاد مسار إلى عقدة الهدف وذلك من خلال بث رسالة طلب توجيه في الشبكة على شكل بث عام (broadcast route request packet RREQ) كما هو موضح في الشكل (2-17)، حيث تتلقى العقد المجاورة الطلب وتقوم بإعادة إرساله وهكذا حتى يصل الطلب إلى عقدة الهدف D.



الشكل (2-19) عملية بث طلب التوجيه RREQ

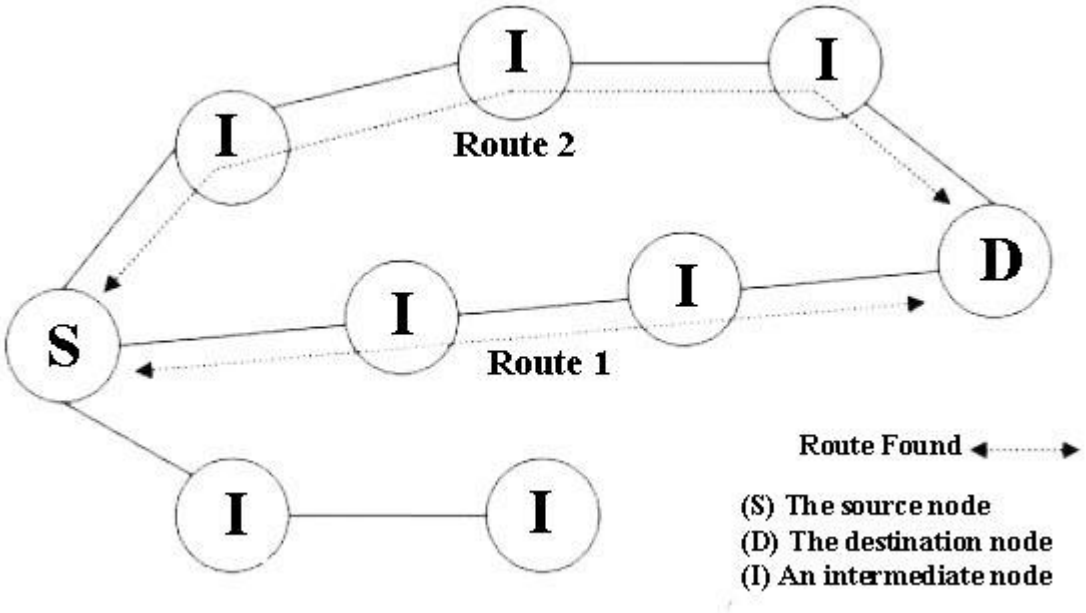
تقوم عقدة الهدف D بإنهاء مرحلة اكتشاف المسار وذلك من خلال إرسال رسالة رد لطلب التوجيه (route reply packet RREP) كما هو موضح في الشكل (2-17).



الشكل (2-20) عملية الرد لطلب التوجيه RREP

عند انتهاء مرحلة اكتشاف المسار قد يكون هناك أكثر من مسار متوفر نحو الوجهة المطلوبة كما يوضح المثال في الشكل (2-18)، في هذه الحالة تقوم العقدة المصدر باختيار المسار الأفضل من بين المسارات المتاحة وفقاً لخوارزمية التوجيه المستخدمة، على سبيل المثال تختار بعض البروتوكولات المسار الأفضل وفقاً لعدد القفزات hop counts الأقل على اعتبار أنه يمثل أقل تكلفة من وجهة نظرها.

حيث يوضح الشكل (2-18) اختيار عقدة المصدر S المسار الأول (Route 1) ذو عدد القفزات الأقل، فيما يمكن أن تعتمد بعض البروتوكولات على عرض الحزمة المتاح bandwidth في اختيار المسار الأفضل.



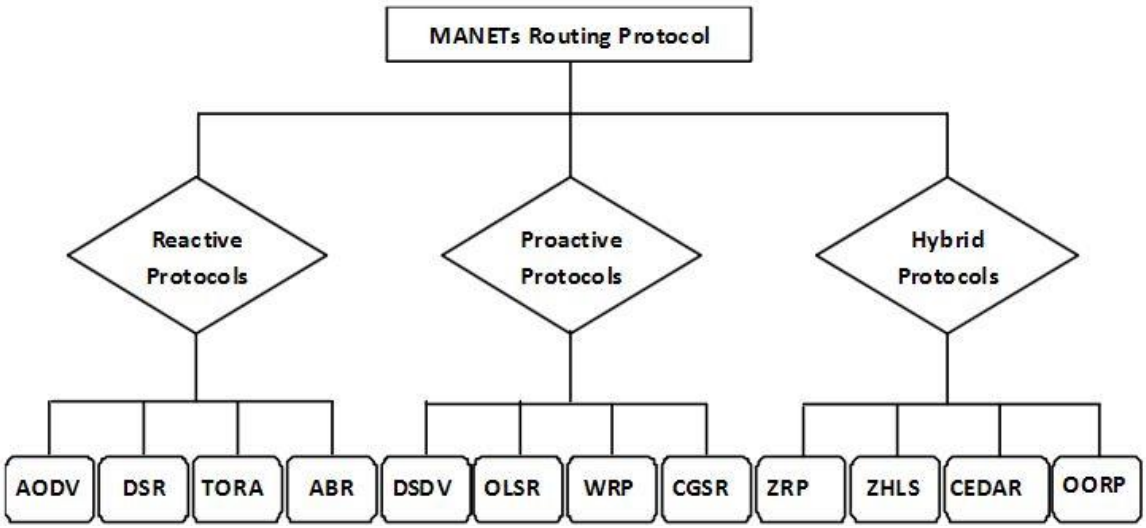
الشكل (2-21) المسارات المتوفرة باتجاه الهدف D

بعد اكتشاف المسارات إلى الوجهة المطلوبة واختيار المسار الأفضل يتم إنشاء هذا المسار وتبدأ هنا المرحلة التالية وهي مرحلة إرسال البيانات Data Forwarding، في هذه المرحلة تتصل العقد الموجودة على المسار مع بعضها البعض، وفي حال حدوث انقطاع لإحدى الوصلات الفعالة على المسار يتم إيقاف الإرسال وتقوم العقدة الأخيرة التي حصل عندها الانقطاع بإبلاغ العقد الأخرى الموجودة على المسار بوجود حالة الانقطاع، أي بمعنى آخر أنه كلما تغيرت طوبولوجيا الشبكة يزداد احتمال حدوث الانقطاع مما ينتج عنه تكرار أكثر لمراحل دورة التوجيه.

2-4-5 بروتوكولات التوجيه في شبكات MANETs:

يتم تصنيف بروتوكولات التوجيه في شبكات MANETs وفقاً للعديد من الاعتبارات وسوف نعتمد هنا في تصنيف بروتوكولات التوجيه وفقاً لاستراتيجية التوجيه، وبذلك يتم تصنيف بروتوكولات التوجيه ضمن ثلاث فئات أساسية وهي

بروتوكولات التوجيه الاستباقية Proactive Routing Protocols، بروتوكولات التوجيه التفاعلية Reactive Routing Protocols وبروتوكولات التوجيه الهجينة Hybrid Routing Protocols، ويوضح الشكل (2-19) أمثلة لأشهر البروتوكولات المستخدمة ضمن كل فئة.



الشكل (2-22) الأنواع الرئيسية لبروتوكولات التوجيه في شبكات الـ MANETs

2-4-5-1 بروتوكولات التوجيه الاستباقية Proactive Routing Protocols:

وتُسمى أيضاً بالبروتوكولات المُقادة بالجدول (table driven) حيث يتم تبادل معلومات التوجيه بين جميع عقد الشبكة ويتم اتخاذ قرار التوجيه بغض النظر عن حاجة الشبكة لها، فهي تستهلك حجماً كبيراً من عرض الحزمة إلا إنها تؤمن سهوله في الحصول على معلومات التوجيه بشكل دائم وبشكل أسرع من التوجيه التفاعلي، لكن هناك صعوبة في تعديل جدول التوجيه في حال فشل إحدى العقد، وتُعتبر هذه البروتوكولات مناسبه من أجل شبكات بعدد محدد من العقد وذلك بسبب التحديثات المتكررة التي تسبب حملاً إضافياً على الشبكة، وتُصَنف هذه البروتوكولات حسب آلية عملها إلى نوعين وهما: distance vector, link state [23].

تتصف هذه البروتوكولات بتأخير زمني قليل حيث إن معلومات التوجيه تكون جاهزة بشكل دائم كما أنها تستجيب بشكل مستمر لتغيرات بنية الشبكة من خلال تحديث جداول التوجيه بشكل دوري حيث تحتفظ بقوائم محدثة للمسارات لأجل كل وجهه في كامل الشبكة من خلال احتساب المسارات إلى كل العقد سواءً لزمت أم لم تلزم، بالإضافة إلى ذلك فأن أي تغيير يطرأ على أحد العقد ينتشر عبر كامل الشبكة وإلا سوف تبقى معلومات التوجيه لبعض العقد قديمة وغير مُحدثة مما يؤدي إلى فشل الاتصال، ولكن من ناحيه أخرى تُعتبر هذه البروتوكولات مستهلكه لموارد الشبكة وتسبب

زيادة حمل التوجيه routing overhead بشكل كبير، بالإضافة إلى اشغال جداول التوجيه مساحة كبيرة من حجم الذاكرة المحدودة، وأهم مميزات هذه البروتوكولات:

- تمتلك كل عقدة جدول توجيه من أجل البث لجميع العقد ضمن الشبكة وتأسيس اتصال مع العقد الأخرى في الشبكة.
- تسجل العقدة كل الوجهات الموجودة ضمن الشبكة، وعدد القفزات المطلوبة للوصول إلى كل وجهه في جدول التوجيه.
- يتم تمييز مدخل جدول التوجيه برقم تسلسلي مولد من قبل العقدة الوجهة.
- يتم تحديث جدول التوجيه كل فترة زمنيه محدده بهدف الحصول على صوره صحيحة عن طوبولوجيا الشبكة وذلك تبعاً للبروتوكول المستخدم، أي تُحدِث عقد الشبكة حالة الشبكة وتحافظ على المسار بغض النظر أكان هناك حركة بيانات أم لا.
- أشهر هذه البروتوكولات: Destination Sequenced Distance Vector (DSDV)، Wireless Routing Protocol (WRP).

2-4-5-2 بروتوكولات التوجيه التفاعلية Reactive Routing Protocols:

وهي بروتوكولات توجيه تقوم بإجراء عمليات التوجيه في الشبكة عند الطلب On demand، أي إن مسارات التوجيه لا تُبنى إلا عند الحاجة فقط، وبالتالي تعمل على توفير عرض الحزمة وينخفض حمل التوجيه routing overhead في الشبكة بشكل كبير، لكن هذا الأمر يزيد من التأخير في عملية توجيه الرزم ضمن الشبكة حيث لا تقوم العقد بإنشاء المسارات ضمن الشبكة إلا عند الحاجة إليها فعلياً، ويتم ذلك من خلال إرسال عقدة المصدر طلب توجيه Route Request (RREQ) لعقد الجوار، وتتميز هذه البروتوكولات بما يلي [24]:

- تُحدَد المسارات عند الطلب من قبل المنبع الذي يقوم بعملية اكتشاف المسار.
- يحدث اكتشاف المسارات دائماً عن طريق غمر الشبكة برزم طلب المسار.
- تخفيض الحمل الزائد المُلاحظ في البروتوكولات الاستباقية (Proactive) عن طريق الاحتفاظ بالمسارات الفعالة فقط.
- إن تحديد المسارات والمحافظة عليها مطلوب من أجل إرسال المعلومات إلى الوجهة الفعلية.
- توجد استراتيجيتان أساسيتان تعمل بهما كل البروتوكولات التفاعلية وهما: Source routing، Hop-by-hop ويوضح الجدول التالي الفرق بينهما:

Source routing	Hop-by-hop routing
كل رزمة معلومات تحتوي العنوان الكامل من المنبع إلى الهدف	كل رزمة معلومات تحوي عنوان الهدف وعنوان القفزة التالية فقط
توجه العقد الوسيطة هذه الرزم اعتماداً على المعلومات الموجودة في ترويسة كل منها	توجه العقد الوسيطة هذه الرزم اعتماداً على جدول توجيهها
تقلل من حجم الحمل الزائد لأن العقدة لا تحتاج للاحتفاظ بالاتصالية مع الجيران باستخدام رسائل Hello	مناسبة للشبكات الديناميكية لأن العقد ستحدث جداولها بشكل دوري
ينخفض أداءها في الشبكات الكبيرة بسبب عدد العقد الوسيطة الكبير الذي يزيد من احتمال حدوث فشل في المسار ويزيد من حجم الحمل الزائد	يجب أن تحتفظ كل عقدة وسيطة بمعلومات التوجيه حول كل مسار فعال وهذا ما يتطلب منها معرفة جيرانها عن طريق إرسال المزيد من الرسائل
أشهرها البروتوكول **DSR**	أشهرها البروتوكول **AODV**

الجدول (2-3) مقارنة بين تقنيات البروتوكولات التفاعلية

2-4-5-3 بروتوكولات التوجيه الهجينة Hybrid Routing Protocols:

وهي البروتوكولات التي تدمج بين فكرتي البروتوكولات الاستباقية (Proactive) والتفاعلية (Reactive)، حيث أن معظمها بروتوكولات معتمدة على تقسيم الشبكة إلى عدد من المناطق أو من العناقيد أو الأشجار[5]، وتعتمد على الاحتفاظ بالمسارات بشكل مسبق للعقد القريبة من بعضها البعض (داخل نفس المنطقة مثلاً) وتحديد المسارات للعقد البعيدة بشكل تفاعلي، أي أن عملها هجين بين الطريقتين السابقتين حيث تُستخدَم البروتوكولات Proactive عندما نريد تقليل التأثير في الشبكات الصغيرة، وتُستخدَم البروتوكولات Reactive في الشبكات الأكبر لتخفيف عبئ المعالجة الزائدة للبيانات، وأشهرها هما البروتوكولين: Zone Routing Protocol (ZRP), Zone-based Hierarchical Link State (ZHLS) [25].

3 الفصل الثالث

بروتوكول التوجيه AODV

Ad hoc On-demand Distance Vector

3-1 مقدمة:

البروتوكول Ad Hoc On-demand Distance Vector Protocol (AODV) هو عبارة عن بروتوكول توجيه تفاعلي (Reactive)، يوصف بأنه بروتوكول توجيه عند الطلب On-demand أي يقوم بتحديد المسار فقط عند الحاجة، ويجمع هذا البروتوكول بين خوارزميتي التوجيه Destination Sequenced Distance Vector (DSDV) الاستباقية وخوارزمية التوجيه Dynamic Source Routing (DSR) التفاعلية، وذلك من خلال الجمع بين محاسن الخوارزميتان معاً، حيث يعتمد مبدأ التوجيه من عقدة إلى عقدة hop-by-hop وآلية الترقيم التسلسلي sequence numbers المُقتبَستان من البروتوكول الاستباقي DSDV علماً أن مبدأ التوجيه من عقدة إلى عقدة يلغى الحاجة لتضمين كامل المسار ضمن ترويسة الرزمة والرقم التسلسلي يُستخدم لتجنب حلقات التوجيه routing loops وتحديد عمر أو حداثة المسار freshness، ومن ناحية أخرى فأن عملية اكتشاف المسار وصيانة هذا المسار عند الحاجة مُقتبسة من البروتوكول DSR.

أهم ما يميز البروتوكول AODV هي قدرته على رسائل التحكم في الشبكة من خلال إنشاء المسارات على أساس الحاجة فقط بدلاً من الاحتفاظ بجدول كامل لكل وجهه في الشبكة وهذا ما يجعل منه تقنية عالية الفعالية في شبكات MANETs، حيث يتكيف هذا البروتوكول مع تغّير الوصلات وفي حال فشل الوصلة يتم إرسال رسائل الإعلام بالفشل إلى العقد المتأثرة فقط في الشبكة، مما يسمح لهذه العقد بتحويل مسارات التوجيه عن الوصلات الفاشلة إلى العقد الفعالة في الشبكة، وبالتالي ضمان موثوقية الشبكة، ويمكن تقسيم العمليات التي ينجزها إلى: اكتشاف المسارات (Routes Discovery) وصيانة المسارات (Routes Maintenance) [26].

3-2 تطبيقات البروتوكول AODV:

تم تصميم البروتوكول **AODV** للعمل في الشبكات النقالة **MANETs** بمختلف الأحجام والكثافات والتي تتراوح بين العشرات وحتى آلاف العقد الثابتة أو المتحركة، ويمكن لهذا البروتوكول التعامل مع حركية بسرعات منخفضة أو متوسطة وحتى السرعات المرتفعة نسبياً، بالإضافة إلى تكيفه مع سرعات متعددة لتدفق البيانات، والهدف الأساسي من هذا البروتوكول هو تقليل تكاليف عمل الشبكة من خلال تقليل انتشار رسائل التحكم وتخفيف حمل التوجيه الزائد **routing overhead** مقارنة مع البروتوكولات التفاعلية الأخرى بهدف تحسين الأداء وتحقيق إمكانية التوسع بشكل موثوق وآمن.

3-3 رسائل البروتوكول AODV:

يُعرّف البروتوكول AODV ثلاثة أنواع من الرسائل وهي كالتالي: Route Requests (RREQs), Route Replies (RREPs), Route Errors (RERRs) ويتم استقبال هذه الرسائل وترويسة IP المعروفة (جميع رسائل البروتوكول AODV تُرسل على البوابة ذات الرقم 654 باستخدام الوكيل UDP)، أي على سبيل المثال تستخدم العقدة المرسلة للطلب عنوانها الخاص IP كعنوان المصدر في الرسالة بينما يُستخدم العنوان الخاص 255.255.255.255 لرسائل البث العام، هذا يعني أن رسائل البروتوكول AODV **لا تنتشر بشكل أعمى في الشبكة وبشكل عام فأن آلية عمل البروتوكول AODV لا تستدعي انتشار بعض الرسائل (مثل RREQ) على نطاق واسع في الشبكة بل على العكس يُحدد نطاق الانتشار لمثل هذه الرسائل بالحقل TTL في ترويسة IP.**

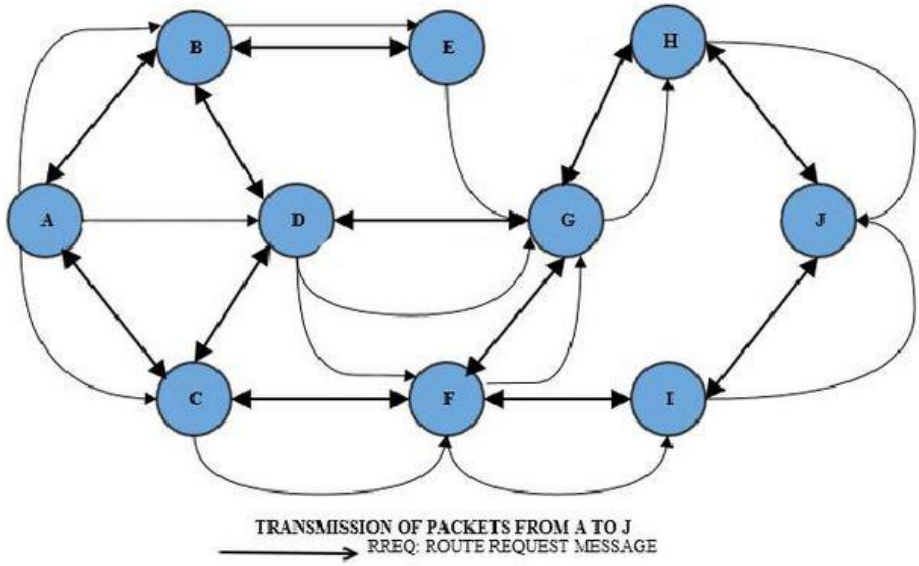
يتولى البروتوكول AODV إدارة جداول التوجيه، بحيث يتوجب الاحتفاظ بمعلومات جدول التوجيه حتى لأجل المسارات ذات زمن الحياة القليل كما في حالة الحقول المؤقتة التي يتم إنشاؤها لحفظ المسارات العكسية نحو العقد المُرسِلة المولدة لطلبات التوجيه RREQs.

3-4 عملية اكتشاف المسار AODV- Route Discovery:

عندما تحتاج عقدة ما من عقد الشبكة إرسال بيانات إلى عقدة أخرى فإنها تتفحص جدول التوجيه الخاص بها بحثاً عن مسار ما إلى الوجهة المطلوبة، ففي حال وجود مسار فعال Active للوجهة المطلوبة تبدأ عقدة المصدر مباشرة بإرسال رزم البيانات إلى العقدة التالية على المسار باتجاه عقدة الهدف، أما في حال عدم توفر أي مسار ضمن جدول التوجيه للعقدة هنا تبدأ عقدة المصدر عملية اكتشاف للمسار، ويتم ذلك من خلال إنشاء طلب توجيه Route Request (RREQ)، حيث أن هذا الطلب هو عبارة عن رسالة تحكم تُرسَل على شكل بث عام (broadcast) كما يوضح الشكل (3-1)، وتتضمن هذه الرسالة المعلومات التالية:

- عنوان المصدر Source IP Address (SIP).
- الرقم التسلسلي للمصدر Source Sequence Number (SSN).
- عنوان الهدف Destination IP Address (DIP).
- آخر رقم تسلسلي معلوم للهدف Last known Destination Sequence Number (DSN).
- معرف البث العام Broadcast ID (BID).
- **عدد القفزات** hop-counts

وفي كل مرة تقوم فيها عقدة المصدر بإرسال طلب توجيه جديد يتم زيادة الرقم **BID** لهذه العقدة، بالتالي فإن الثنائية المكونة من **BID** و**SIP** تُستخدَم لتعريف طلب توجيه **RREQ** وحيد للمرسل.



الشكل (3–1) انتشار رزمة طلب المسار RREQ للبروتوكول AODV

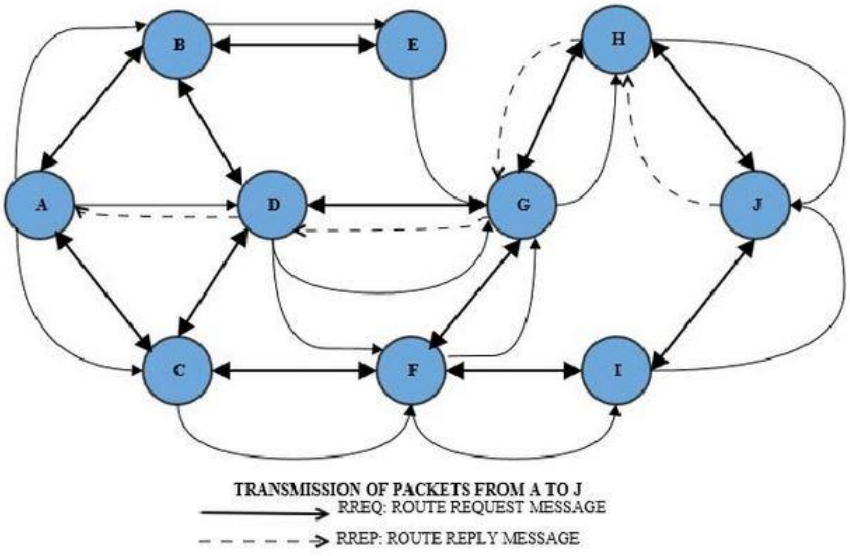
حالما يتم إنشاء طلب التوجيه RREQ تقوم عقدة المصدر بإرساله لكل عقد الجوار كما يوضح الشكل (3–2) وتشغّل مؤقتاً بانتظار الرد.

يتضمن طلب التوجيه كما ذكرنا سابقاً رقمين تسلسليين لكل من المصدر والوجهة، بحيث يحدد الرقم التسلسلي للمصدر Source Sequence Number حداثة المسار العكسي Reverse Path، بينما يحدد الرقم التسلسلي للهدف destination Sequence Number آخر معلومة لدى المرسل عن حالة عقدة الهدف.

يُنشر طلب التوجيه تباعاً في الشبكة حتى يصل إلى الوجهة المطلوبة ذاتها أو إلى إحدى العقد الوسيطة التي تملك مساراً حديثاً نحو الوجهة المطلوبة، حيث أنه عندما تستقبل عقدة ما رسالة طلب المسار RREQ وإذا لم تكن هي العقدة الهدف ولم تتلقى نسخة من هذا الطلب من قبل فأنها تقوم بإعادة بث هذا الطلب لكل جيرانها بعد أن تسجل ضمن جدول توجيهها المعلومات التالية: عنوان المصدر، عنوان الهدف، الرقم التسلسلي للهدف، عدد القفزات بعد زيادتها بمقدار واحد، وبذلك يتشكل المسار العكسي Reverse Path، علماً أن كل عقدة وسيطة تستقبل رزمة الطلب الأولى فقط الخاصة بمصدر وهدف محددين وكل نسخة أخرى يتم إهمالها [27].

أما في حال كانت العقدة المُستقبلة لرسالة طلب المسار RREQ هي العقدة الهدف هنا تقوم هذه العقدة بأنها عملية الطلب وإرسال رسالة إجابة Route Reply (RREP) إلى المصدر بعملية بث أحادي unicast باستخدام المسار

العكسي Reverse Path المشكل مسبقاً كما هو موضح بالشكل (3-2)، وتتضمن هذه الرسالة المعلومات التالية: الرقم التسلسلي للهدف Destination Sequence Number (DSN)، عدد القفزات (بعد تصفيرها) hop-counts، وزمن حياة المسار Time To Life (TTL).



الشكل (3-2) انتشار رزمة إجابة المسار RREP للبروتوكول AODV

عندما تستقبل العقدة الوسيطة رسالة الإجابة تقوم بتسجيل المعلومات التالية: عنوان الهدف، العقدة المجاورة التي تلقت منها الرزمة، عدد القفزات، زمن الحياة، وبذلك يتشكل المسار الأمامي Forward Route والذي سوف تستخدمه العقدة المصدر لإرسال البيانات Data إلى الهدف وذلك عند تلقيها لأول رسالة إجابة RREP.

بعد ذلك في حال تلقي العقدة المصدر رسالة إجابة بعدد قفزات أقل تقوم بتعديل المسار إلى المسار الجديد، وتحتفظ كل عقدة بعداد لزمن الحياة TTL للمسار بحيث تقوم بحذف تسجيل المسار بعد انقضاء زمن محدد من عدم استخدام هذا المسار وهو عادة 300 ثانية.

3-5 عملية صيانة المسار AODV- Route Maintenance:

يتم المحافظة على المسار بين المصدر والوجهة طالما تحتاجه عقدة المصدر، ويمكن لعقدة المصدر أن تبدأ عملية جديدة لاكتشاف المسار في حالة انقطاع الوصلة نتيجة حركة هذه العقدة، ولكن من ناحية أخرى قد يحصل انقطاع في المسار نتيجة لحركة عقدة وسيطة وفي هذه الحالة تقوم العقدة التي اكتشفت هذا الانقطاع بتوليد رسالة خطأ Route Error (RERR) وإرسالها باتجاه عقدة المصدر، بحيث تتضمن هذه الرسالة لائحة بكل الوجهات المتأثرة الوصلة والتي لم يعد بالإمكان الاتصال بها، عندما تستقبل إحدى عقد الجوار رسالة الخطأ المرسلة RERR فإنها تقوم بتفحص

جدول التوجيه الخاص بها بحثاً عن عناوين الوجهات المضمنة في رسالة الخطأ لتشير إلى هذه العناوين بأنها غير صالحة invalid وتحدد المسافة إليها بعدد لانهائي من القفزات.

تتضمن عملية صيانة المسار آلية لاكتشاف حالات انقطاع الوصلة، تعتمد هذه الآلية على تبادل رسائل الترحيب Hello messages لضمان الاتصال المحلي مع عقد الجوار، ويتم تبادل هذه الرسائل بشكل دوري لضمان استمرارية الاتصال مع العقدة التالية [28].

3-5-1 رسائل الترحيب Hello messages:

تعاني شبكات MANETs مثل معظم الشبكات اللاسلكية من مشكلة انقطاع الوصلة بشكل متكرر، وتحدث هذه الانقطاعات نتيجةً لعوامل عديدة مثل حركية العقد، العوائق الفيزيائية، محدودية مصادر الطاقة، التخامد، التداخل، محدودية عرض الحزمة، وجميع هذه العوامل تجعل هذه الشبكات عرضةً لانقطاعات متكررة مما يؤدي إلى تدهور الأداء في الشبكة وانخفاض وموثوقيتها.

بناءً على ذلك تصبح مسألة تحقيق أداء وموثوقية مقبولين في ظروف انقطاعات الوصلة في الشبكات الديناميكية تحدياً حقيقياً.

وبالتالي يُفتَرض تكون الخطوة الأولى في تجنب أثر انقطاع الوصلة هي تحديد وكشف حالات الانقطاع بدقة وسرعة كافية، وتوجد آليتين لكشف انقطاعات الوصلة حيث تعتمد الطريقة الأولى على استخدام تغذيه راجعة Link Layer Feedback تجمع بين طبقة MAC وطبقة الشبكة Network، بينما تعتمد الطريقة الثانية على استخدام رسائل الترحيب Hello Messages.

بالرغم من أن طريقة التغذية الراجعة هي الأسرع في كشف انقطاع الوصلة إلا أن طريقة رسائل الترحيب هي الأكثر شيوعاً حيث أنها تتطلب موارد أقل من حيث الذاكرة والطاقة وهي أسهل للتنفيذ ضمن بروتوكولات التوجيه وأكثر موثوقية من طريقة التغذية الراجعة التي تسبب في بعض الأحيان إنذارات خاطئة متكررة نتيجة لتفسير حالات الانقطاع الآنية على أنها انقطاعات دائمة.

أغلب شبكات MANETs هي عباره شبكات ديناميكية تتغير فيها الطوبولوجيا باستمرار نتيجةً لحركة العقد، وبالتالي تصبح مسألة الحصول على معلومات الجوار بدقة عنصراً أساسياً في تحديد أداء الشبكة، يؤمن البروتوكول AODV معلومات الجوار عن طريق استخدام رسائل **التعارف** Hello Messages.

رسالة الترحيب Hello message هي عبارة عن رسالة إجابة RREP ذات قيم الحقول التالية: عنوان الوجهة (DIP) هو عنوان العقدة الحالية، الرقم التسلسلي للوجهة (DSN) هو آخر رقم تسلسلي للعقدة الحالية، عدد القفزات هو صفر، زمن الحياة يُعطى بالجداء التالي ALLOWED_HELLO_LOSS*HELLO_INTERVAL.

تُرسَل رسائل الترحيب كما يلي:

- لأجل كل فترة زمنية مساوية للقيمة (HELLO_INTERVAL ms) تتفحص العقدة فيما إذا كانت قد سبق وأرسلت أي رسالة بث عام broadcast خلال HELLO_INTERVAL السابقة، وإذا لم تكن قد قامت بأي عملية broadcast خلال هذه المدة فإنها ترسل رسالة تعارف للدلالة على وجودها.
- عندما تستقبل أي عقدة رسالة التعارف من إحدى عقد الجوار، فإنها إما تنشأ أو تحدّث حقل عقدة الجوار هذه في جدول التوجيه لديها.
- إذا انقضت مدة زمنية مساوية للمدة ALLOWED_HELLO_LOSS*HELLO_INTERVAL بدون ورود رسالة تعارف أو غيرها من عقدة الجوار عندها يُعتبَر الاتصال مع هذه العقدة مفقوداً.

من الواضح أن أداء عملية تحديد الجوار وكشف حالات الانقطاع باستخدام رسائل التعارف يعتمد على قيمة المعاملين: ALLOWED_HELLO_LOSS وHELLO_INTERVAL.

حيث يحدد المعامل HELLO_INTERVAL الدور الزمني الأعظمي بين عمليات إرسال رسائل التعارف، وتكون القيمة الافتراضية له مساوية 1 ثانية في البروتوكول AODV، حيث أن القيم المنخفضة لهذا المعامل تسرّع عملية التعرف على الجوار وكشف الانقطاعات وبالتالي إمكانية بناء جداول جوار دقيقة، ولكن من ناحيه أخرى تؤدي الأدوار الزمنية المنخفضة إلى ارتفاع الحمل الزائد Overhead مما يزيد من استهلاك طاقة العقد ويزيد من الاختناقات في الشبكة ويسبب انخفاض الإنتاجية Throughput، أما القيم المرتفعة لهذا المعامل تخفف الاختناقات الناتجة عن الحمل الزائد ولكنها تبطئ سرعة الاستجابة لتغيرات الشبكة وتؤدي بالنتيجة إلى بناء جداول جوار منخفضة الدقة.

يحدد المعامل ALLOWED_HELLO_LOSS العدد الأعظمي المسموح به من رسائل التعارف المفقودة قبل أن يتم تحديد عقدة الجوار كعقدة غير متاحة (أي حالة انقطاع مسار)، ويأخذ هذا المعامل القيمة 2 كقيمة افتراضية في البروتوكول AODV، وقد يؤدي ضبط هذا المعامل إلى القيمة الوحيدة الأدنى وهي 1 إلى انخفاض الأداء أحياناً لان عقد الجوار قد تضيع رسائلها نتيجةً لظروف اتصال سيئة مؤقتة وبالتالي سيتم اعتبارهم غير متاحين، ومن ناحية أخرى يؤدي رفع قيمة هذا المعامل لقيمة أعلى إلى انخفاض في الأداء نتيجة بطيء الاستجابة لتغيرات الشبكة.

4 الفصل الرابع

الأمن في شبكات MANETS

(Security in MANETs)

4-1 الهجمات الأمنية في شبكات MANETs:

دعت الحاجة نتيجة الطلب المتزايد على استخدام هذا النوع من الشبكات لجعلها آمنة، الأمر الذي يعتبر تحدياً يصعب تحقيقه بسبب خصائص هذا النوع من الشبكات، حيث تعتبر هذه الشبكات عرضة للعديد من الهجمات بسبب طبيعة الاتصال اللاسلكي، ومن هذه الهجمات هجوم الرجل في الوسط Man-in-the Middle attack أو هجوم الانتحال Spoofing attack أو هجوم إعادة إرسال الرسائل Replaying attack، حيث أن وسط الاتصال اللاسلكي وسط مفتوح ومحدود الأمن الفيزيائي ومتاح للجميع ويمكن اختراقه والتنصت عليه، على خلاف وسط الاتصال السلكي والذي يحتاج أن يكون المهاجم لديه وصول مباشر للجهاز الشبكي أو أن يقوم بثقب كبل الاتصال لتنفيذ أحد الهجمات السابقة.

أما في شبكات MANETs فإن المهاجم يمكنه التنصت على كافة الرسائل المرسلة ضمن مجال الاتصال الراديوي له،

وذلك من خلال العمل في الوضع Promiscuous mode واستخدام هوائي موجه وبرنامج لتحليل الطرود، وكمثال على أحد أدوات المراقبة واختراق الشبكات اللاسلكية برنامج Ethereal حيث يكفي أن يكون المهاجم ضمن مجال الاتصال الراديوي ليقوم باعتراض الرزم المرسلة بدون معرفة المرسل والقيام بتعديلها وإعادة إرسالها مع أنها مرسلة من جهة غير مخولة بذلك.

كذلك بسبب محدودية عرض حزمة وسط الاتصال فإن المهاجم يمكنه اشغال الوسط بإرسال رزم تحكم إضافية في الشبكة واستغلال القناة أو القيام بالتشويش Jamming عليها.

4-2 تصنيف الهجمات الأمنية في شبكات MANETs:

يمكن تصنيف الهجمات في شبكات MANETs وفقاً لعدة معايير مثلاً يمكن أن تُصنَف الهجمات حسب فعالية الهجوم ومدى تأثيره على الشبكة فيما إذا أدى إلى تعطيل الشبكة أم لا إلى هجوم غير فعال Passive Attack وهجوم فعال Active Attack، أو يمكن أن تُصنَيف الهجمات الأمنية التي تتعرض لها هذه الشبكات حسب الطبقة التي يستهدفها الهجوم من طبقات النموذج OSI بدءً من الطبقة الفيزيائية Physical Layer ووصولاً لطبقة التطبيقات Application Layers ويمكن أن يُنفَذ الهجوم على عدة طبقات معاً، أو تبعاً لنموذج التهديد الذي ينفذه المهاجم إما هجوم داخلي أو خارجي [30] [29].

4-2-1 تصنيف الهجمات حسب فعالية الهجوم ومدى تأثيره:

4-2-1-1 هجوم سلبي وغير فعال Passive Attack:

في هذا النوع من الهجوم يحاول المهاجم الحصول على معلومات قّيمة من الشبكة وذلك من خلال التنصت على معلومات التوجيه Eavesdropping ومراقبتها Monitoring وتحليلها Analysis Traffic للاستفادة منها، وكل ذلك يتم دون أن يتم تعطيل أو التأثير على عمل بروتوكول التوجيه، حيث أن المعلومات التي يحصل عليها المهاجم قد تكشف معلومات مهمة عن علاقة العقد ببعضها البعض أو قد تكشف معلومات عن بنية الشبكة وعناوين العقد ومواقعها،

على سبيل المثال عندما يتم طلب مسار لعقدة ما عدة مرات متتالية عندما يمكن للمهاجم أن يتوقع بأن تلك العقدة تؤدي وظيفة ودوراً هاماً في الشبكة، وبالتالي تعطيل عملها قد يؤدي إلى تعطيل وانهيار كامل الشبكة [29].

يمكن تنفيذ هذا النوع من الهجوم باستخدام عقد سيئة من داخل الشبكة Malicious Nodes وذلك من خلال تجاهل المهام الموكلة إليها، مثل تجاهل الرزم Silent Discard أو إخفاء بعض معلومات التوجيه أو التنصت على القناة ومحاولة جمع بعض المعلومات القيمة.

يتميز هذا النوع من الهجوم بأن المهاجم يتمكن من اختراق وسط الاتصال اللاسلكي دون أن يتم اكتشافه، وهنا تكمن صعوبة تطبيق الخدمات الأمنية لمواجهة هذا النوع من الهجمات.

4-2-1-2 هجوم نشط وفعال Active Attack:

يعتمد هذا الهجوم على تعطيل بعض وظائف الشبكة مثل التعديل على سير عمل بروتوكول التوجيه المستخدم أو تعطيل وظائف بعض العقد، ومن أمثلة هذه الهجمات: هجوم انكار الخدمة Denial of Service Attack (DOS)، هجوم تعديل الرسائل وحذفها Modification/Deletion، هجوم انتحال هوية العقد Impersonation، تزوير الرسائل Fabrication، إعادة إرسال الرسائل Replaying.

قد يستخدم المهاجم في هجماته خاصية التخفي لإخفاء آثار هجومه إما من قبل الشخص المُراقب للنظام أو من نظام اكتشاف الاختراقات Intrusion Detection System (IDS)، ويمكن اكتشاف هذا النوع من الهجمات والتصدي لها [29].

4-2-2 تصنيف الهجمات حسب الطبقة المُستهدَفة [31]:

4-2-2-1 الهجوم في الطبقة الفيزيائية Physical Layer Attacks:

هجوم التنصت هو اعتراض وقراءة الرسائل من قبل الأشخاص غير مخولين بقراءتها، وبما أن معظم الاتصالات اللاسلكية تستخدم المجال الراديوي للإرسال والاستقبال، فيمكن باستخدام هوائي مستقل مضبوط على تردد العمل للشبكة اعتراض الرسائل المرسلة وإقحام رسائل مزورة أو مزيفة في الشبكة.

كما يمكن التشويش Jamming على الإشارات الراديوية والتي تؤدي بدورها إلى ضياع الرسائل وتخريبها، ويتم ذلك من خلال استخدام هوائي مُرسِل قوي يستطيع توليد إشارات تتفوق على الإشارة المرسلة وتسبب لها التشويش، ويكمن تنفيذ هذا الهجوم من مكان بعيد عن الشبكة المستهدفة [31].

4-2-2-2 الهجوم في طبقة وصلة البيانات Data Link Layer Attacks:

تتميز شبكات MANETs بإن العقد المكونة لها تتشارك بوسط النقل اللاسلكي المفتوح للكل، وتحقق هذه الطبقة مهمة الاتصال الند للند peer to peer، أما طبقة الشبكة تؤمن الاتصال بين العقد البعيدة في الشبكة، إن الهجمات التي تستهدف طبقة التوصيل تقوم بتعطيل التعاون اللازم لعمل البروتوكولات في هذه الطبقة مثل التأثير على معيار الاتصال IEEE 802.11.

4-2-2-3 الهجوم في طبقة الشبكة Network Layer Attacks:

تؤمن بروتوكولات طبقة الشبكة الاتصال بين العقد البعيدة وذلك من خلال ما يُعرَف بالاتصال متعدد القفزات الذي يقوم على التعاون القائم بين عقد الشبكة.

تمت دراسة الهجمات التي تستهدف طبقة الشبكة في العديد من الأبحاث، حيث يتمكن المهاجم من مهاجمة بروتوكولات التوجيه الموجودة في هذه الطبقة والتغيير في آلية عملها، وإقحام نفسه في الطريق بين المصدر والهدف وبالتالي التحكم بتدفق الرزم المتبادلة بينهما.

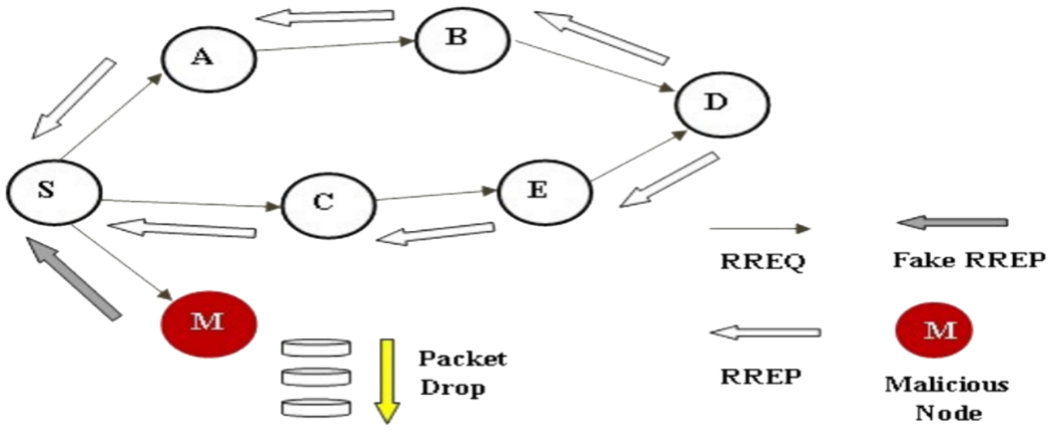
يمكن للرزم أن تُرسل عبر طريق غير أمثلي الأمر الذي من شأنه توليد تأخير في زمن الأرسال، كما يمكن للرزم أن توجه عبر مسار غير موجود الأمر الذي يسبب ضياعها، كما يمكن للمهاجم أن يشكل حلقات توجيه مما يتسبب باختناق شديد في الشبكة واستنزاف في مواردها المحدودة وتنافس على القناة في بعض المجالات، كما يمكن لعدة عقد متعاونة مجتمعة القيام بمنع المصدر من إيجاد طريق للعقدة الهدف مسبباً تجزئة وتدهور أداء الشبكة [31].

حيث إن العقد الموجودة في الشبكة هي إما عقد طرفية أو عقد تقوم بوظيفة موجه، وبما أن رسائل التوجيه تُرسل عبر وسط الاتصال اللاسلكي والذي يفتقر إلى الحماية الفيزيائية، لذلك يمكن أن تصبح بعض الطرق غير صالحة وغير مطابقة للطريق الصحيح الذي بتم اكتشافه من قبل البروتوكول بسبب التلاعب في معالجة رسائل التوجيه، وهذا يؤدي في النتيجة إلى انهيار في أداء الشبكة وتعطيل عملها والتأثير عليها بشكل كبير.

قد تستهدف بعض هجمات الشبكة مرحلة اكتشاف المسار وذلك من خلال عدم اتباع آلية عمل بروتوكول التوجيه المستخدَم، لذلك تُعتبَر رسائل التوجيه التي تنتقل في الشبكة والمستخدمة لإعداد الاتصال بين العقد وإنشاء الطريق العنصر الأساسي لشن هذه الهجمات، ويتم تنفيذ هذه الهجمات من قبل عقدة مؤذية Malicious أو عقدة أنانية Selfish، حيث أن العقدة المؤذية Malicious Node تقوم بإساءة التصرف لأن لديها نية أو هدف لإلحاق الضرر بالشبكة وتعطيل عملها، أما العقدة الأنانية Selfish Node تقوم بإساءة التصرف توفيراً لمواردها مثل طاقة البطارية وذلك بتمرير اتصالاتها الخاصة، وعدم مشاركتها في عمل بروتوكول التوجيه أو عدم القيام بتوجيه الرزم التي تمر عبرها، وأهم هجمات التوجيه هي هجمات الثقوب مثل هجوم الثقب الأسود Black Hole، وهجوم الثقب الرمادي Gray Hole، وهجوم الثقب الدودي Worm Hole، وسوف نوضح هذه الهجمات في سياق هذه الدراسة.

- **هجوم الثقب الأسود Black Hole Attack:**

تقوم العقدة الخصم في هذا الهجوم بالرد على طلبات اكتشاف الطريق على الرغم من عدم امتلاكها طريقاً نحو الوجهة، وتستخدم بروتوكول التوجيه لتعلن أنها تملك طريق بكلفة منخفضة باتجاه الهدف، وبذلك استطاعت اقحام نفسها في الطريق المكتشف وبإمكانها بعد أن أصبحت جزءً من الطريق شن أي هجوم ومعالجة رزم البيانات المارة، مثلاً قد تختار حذف الرزم مسببةً هجوم منع الخدمة أو قد تستغل موقعها في الطريق كخطوة أولى في هجوم الرجل في الوسط أو قد تقوم بمقاطعة الطرود وعدم إرسالها وتوجيهها [32].



الشكل (4-1) هجوم الثقب الأسود Black Hole Attack

- **هجوم الثقب الدودي Worm Hole Attack:**

ويسمى أيضاً بهجوم النفق ويشن من قبل عقدتين مؤذيتين متعاونتين ومتآمرتين ومتصلتين بوصلة اتصال سريعة تسمى النفق، حيت تملك كل عقدة منهما وحدتين راديويتين للإرسال، إحدى هاتين الوحدتين يتم استخدامها للتعامل مع عقد الشبكة الأخرى والمشاركة في عمليات اكتشاف المسارات وتوجيه رسائل الشبكة المختلفة، والوحدة الراديوية الأخرى تستخدمها كل من العقدتين للتواصل مع العقدة المهاجمة الأخرى بحيث تعمل على تردد خاص ضمن قناة سرية خاصة تُسمى النفق ولها ميزات متطورة بالنسبة لمدى ومعدل الارسال، حيث تتوضع العقدتان في موقعين متباعدين وتقومان بتنفيذ هجوم حجب الخدمة عن عقد محددة موجودة بينهما من خلال اسقاط كل الرزم الخاصة بهذه العقد المُستهدَفة وتمرير كل رسائل الشبكة الأخرى بشكل طبيعي، وبذلك تعطيان صورة غير صحيحة عن طوبولوجيا الشبكة حيث إن المسارات الأقصر تمر عبرهما [33].

- **هجوم الثقب الرمادي Grey Hole Attack:**

تقوم العقدة الخصم بإسقاط وحذف بعض رزم البيانات التي يتوجب عليها تمريرها وإرسالها للعقد الأخرى ضمن الشبكة، ويتم ذلك بحذف كل أو بعض الرزم الخاصة بعقدة محددة دون غيرها، والهدف الأساسي من هذا الهجوم هو تخفيض نوعية الخدمة المقدمة من الشبكة وزيادة استهلاك وهدر موارد العقد التي تقوم بإرسال الرزم، حيث تشارك العقدة الخصم في مرحلة إعداد الطريق لتكون جزءً منه وبعد ذلك تقوم باستهداف عقدة محددة دون غيرها وتمنعها من تمرير بياناتها.

4-2-2-4 الهجوم في طبقة النقل Transport Layer Attack:

الهدف الأساسي من البروتوكولات الموجودة في هذه الطبقة مثل البروتوكول TCP هو تأمين وإعداد الاتصال من النهاية إلى النهاية end-to-end، بحيث يحقق هذا الاتصال موثوقية في نقل البيانات عبر الشبكة ويؤمن التحكم بالتدفق، والتحكم بالازدحام، ومن ثم إنهاء جلسة الاتصال.

أحد أنواع الهجمات التي تستهدف هذه الطبقة هو هجوم اغراق الشبكة بالطلبات SYN Flooding، وهجوم سرقة الجلسة Session hijacking، وبما أن شبكات MANETs تملك معدل أخطاء أعلى مقارنة مع الشبكات السلكية، وكون بروتوكول TCP لا يملك آلية للتمييز بين ضياع الرزم بسبب الازدحام أو بسبب الأخطاء العشوائية أو نتيجة الأعمال الهجومية، فإنه يقوم بإنقاص حجم نافذة الازدحام CWND عند حدوث الضياع الأمر الذي يؤدي إلى انخفاض كبير وتدهور في أداء الشبكة [31].

أحد أهم الهجمات التي تستهدف طبقة النقل هو هجوم اغراق الشبكة في طلبات الاتصال SYN Flooding Attack ويؤدي هذا الهجوم بدوره إلى هجوم انكار الخدمة Denial-of-service، حيث يقوم المهاجم بتوليد عدد كبير من الاتصالات نصف المفتوحة باتجاه العقدة المُستهدَفة، ولا يكمل عملية المصافحة اللازمة لإتمام عملية فتح الاتصال، حيث كما هو معلوم فأن أي عقدتان ترغبان بالاتصال فيما بينهما فإنه يجب أولاً إعداد الاتصال باستخدام آلية المصافحة الثلاثية Three-way handshake

4-2-2-5 الهجوم في طبقة التطبيقات:

يتم تنفيذ الهجوم في طبقة التطبيقات من خلال نشر الفيروسات Virus أو من خلال هجوم الانكار Repudiation.

- **هجوم الفيروسات Virus Attack:**

تحوي طبقة التطبيقات بيانات المستخدم المرسلة وتدعم هذه الطبقة عدة بروتوكولات مثل HTTP, SMTP, FTP يستغل المهاجم هذه البروتوكولات لتمرير البرنامج المؤذي والذي يحوي الفيروسات بهدف استغلال نظام التشغيل وبعض التطبيقات، يتواجد الكثير من البرامج الخبيثة مثل الفيروسات المنتشرة عبر الانترنت والتي تملك التقنيات التي تمكنها من اكتشاف الأجهزة الجديدة ليتم استغلالها وشن الهجمات عليها، وكمثال على ذلك القيام بمسح العناوين وأرقام البوابات IP and Ports scan الذي تقوم به الفيروسات، ويتم ذلك من خلال إرسال طرود وتوجيهها إلى منافذ أو بوابات Ports مفتوحة واستغلال الثغرات الأمنية الموجودة فيها وذلك مع عناوين IP مختلفة وعندها تستقبل الأجهزة المستهدفة نسخة من البرنامج الضار وبذلك تكون قد أُصيبَت بالعدوى وكمثال على ذلك الفيروسات التي تستخدم آلية المسح Code Red [31].

- **هجوم الانكار Repudiation Attack:**

يتحكم الجدار الناري في طبقة الشبكة بحركة الرزم الداخلة والخارجة من الشبكة، أما في طبقة النقل فإن كافة الاتصالات يمكن تشفيرها من النهاية إلى النهاية end-to-end، ولكن جميع هذه التقنيات لا تقدم حلولاً لمشاكل الانكار بشكل عام، وكمثال على ذلك يمكن للشخص الأناني أن ينكر مشاركته في أي عملية شراء باستخدام بطاقة الائتمان أو أي مناقلات مالية تمت عبر الانترنت، وهذا يُعتبَر النموذج الأساسي لهجوم الإنكار الذي يستهدف الأنظمة التجارية.

4-2-2-6 الهجوم على عدة طبقات Multi-Layers Attack:

يمكن لبعض أنواع الهجوم أن تنفذ من عدة طبقات بدلاً من طبقة واحدة محددة، ومن أشكال هذه الهجمات على سبيل المثال هجوم إنكار الخدمة Denial Of Service (DOS)، وهجوم الرجل في الوسط Man-In-the-Middle Attack (MIMA)، وهجوم انتحال الشخصية Impersonation.

- **هجوم إنكار الخدمة Denial Of Service (DOS):**

يمكن لهذا الهجوم أن يُنفَذ من عدة طبقات، على سبيل المثال يمكن للمهاجم أن يقوم بالتشويش في الطبقة الفيزيائية والذي يؤدي بدوره إلى تعطيل الاتصال، وفي طبقة التوصيل يمكن للعقد المهاجمة أن تشغل القناة وتستولي عليها وتمنع العقد الأخرى من استخدامها، أما في طبقة الشبكة يمكن تعطيل عملية التوجيه من خلال التعديل في رسائل التحكم، وحذف بعض الرسائل دون غيرها، وتعبئة جداول التوجيه مما يسبب فيض جدول التوجيه وتسميم المعلومات الموجودة ضمنه، أما بالنسبة لطبقة النقل وطبقة التطبيقات فينفذ هجوم الفيض في طلبات فتح الاتصال الذي يندرج تحت هذه القائمة من الهجمات حيث يحاول المهاجم استهلاك موارد الشبكة بما فيها طاقة العقدة المحدودة عن طريق إرسال طلبات اكتشاف مسار بهدف اشغال العقد بعمليات الإرسال والمعالجة، وهجوم سرقة الجلسة ونشر البرامج الخبيثة كالفيروسات التي تؤدي بدورها إلى هجوم منع الخدمة.

- **هجوم الرجل في الوسط Man-In-the-Middle Attack (MIMA):**

يتواجد المهاجم على مسار الارسال بين المرسل والمستقبل ويقوم بالتنصت على جميع الرسائل والمعلومات المتبادلة بينهما، وفي بعض الحالات يقوم المهاجم بانتحال هوية المرسل ليتابع جلسة الاتصال مع المستقبل، أو ينتحل هوية المستقبل ليقوم بالرد والإجابة على المرسل.

- **هجوم انتحال الشخصية Impersonation:**

يُعتبر هذا الهجوم الخطوة الأولى لشن هجمات أخرى أكثر تقدماً، حيث يسبق المهاجم أي عمل هجومي بتغيير عنوانه الفيزيائي MAC أو عنوانه الشبكي IP منتحلاً هوية إحدى العقد الموثوقة، وبذلك يمكن لهذه العقدة أن تنضم للشبكة بدون أن تُكتشَف، وقد ترسل معلومات توجيه مزورة وخاطئة، وكمثال على ذلك هجوم الثقب الأسود Black Hole Attack، حيث تستخدم العقدة المهاجمة بروتوكول التوجيه لتعلن عن نفسها أنها تملك أفضل مسار متاح للهدف وبعد ذلك تقوم بحذف البيانات.

4-2-3 تصنيف الهجمات حسب طبيعة المهاجم:

4-2-3-1 الهجوم الخارجي:

يُنفذ هذا الهجوم من قبل عقدة غير مخولة ولا تمتلك حق الوصول للشبكة، حيث تقوم باعتراض الاتصال بين العقد واستخدام قناة الاتصال اللاسلكية للتنصت والتشويش وإقحام رسائل مزيفة والتعديل على حقول رسائل التوجيه أو إعادة إرسالها، وقد تجتمع مجموعة من العقد وتسيطر على الشبكة، ويمكن اكتشاف هذا النوع من الهجوم.

4-2-3-2 الهجوم الداخلي:

يُنفذ هذا الهجوم من قبل عقد من داخل الشبكة، حيث تكون عقد شرعية ومخول لها بالدخول وتمتلك صلاحيات داخل الشبكة، ويُعتبَر هذا النوع من الهجوم صعب الاكتشاف بسبب تنفيذه من قبل عقد موثوقة وبحوزتها المفاتيح الصحيحة، تعتبر شبكات MANETs معرضة لكلا النوعين من الهجوم، وذلك لإن العقد لا تمتلك حماية فيزيائية ولهذا فهي عرضة للسرقة من قبل العقد الخصم أو العدو [31].

4-3 التحديات الأمنية في شبكات MANETs:

تطرح خصائص الأساسية المميزة لهذه الشبكات والتي تم ذكرها سابقاً مجموعة من التحديات الأمنية المتمثلة في النقاط الأربع التالية:

أولاً: بسبب استخدام وسط الاتصال اللاسلكي فإن الشبكة معرضة للعديد من الهجمات التي تستهدف الاتصال وتتراوح من الهجوم غير الفعال كالتنصت وسرقة المعلومات والذي يعرضها للخطر وانتهاك خصوصيتها من قبل المهاجم، إلى الهجوم الفعال المتمثل بحذف الرزم أو إضافة رزم مزورة والتعديل على حقول هذه الرزم بالإضافة إلى انتحال هوية عقدة ما ضمن الشبكة.

ثانياً: تفتقر العقد الموجودة في بيئة عدائية مثل أرض المعركة للحماية الفيزيائية، لذلك فهناك احتمال أن تتم سرقتها والسيطرة عليها والتسبب لضرر فيزيائي لها أو التحكم بها، حيث يجب دوماً الأخذ بعين الاعتبار أن الهجمات يمكن أن تنفذ من قبل عقد من خارج الشبكة وأحياناً من قبل عقد مُسيطَر عليها Compromised node من داخل الشبكة.

ثالثاً: تسبب الطوبولوجيا المتغيرة للشبكة بشكل ديناميكي نظراً لتغير حجم الشبكة وحركة العقد المستمرة إمكانية انضمام أو مغادرة بعض العقد للشبكة بشكل متكرر وفي أي وقت، كما يمكن لعلاقات القة المتبادلة بين العقد أن تتغير عند اكتشاف أحد العقد المهاجمة ضمن الشبكة، لذلك لا يمكن للحل ذو الاعدادات الثابتة أن يكون كافياً بل يجب أن يكون كل حل أمني قادراً على التكيف مع تغيرات الطوبولوجيا.

رابعاً: تشكل محدودية موارد هذا النوع من الشبكات وعرض النطاق الترددي المحدود والوصلات الغير تناظرية عائقاً في وجه الحلول الأمنية، وتشكل المركزية عائقاً في تصميم أي خدمة أمنية في شبكات MANETs لأنها لا تعتمد على وجود أي إدارة مركزية، كما لا يمكن ضمان وجودها في أي وقت نظراً لحركة العقد.

اعتماداً على ما سبق فأن أي بروتوكول أمني أو إضافة أمنية مصممة لشبكات MANETs حتى تكون فعالة يجب أن تحقق بعض الشروط المتمثلة بما يلي:

- توليد عبء معالجة أقل من حيث عمليات التشفير وفك التشفير.

- كفاءه في استخدام عرض حزمة الاتصال وذلك من خلال استخدام الموارد المحدودة بفعالية وكفاءة.
- كلفة الاتصال الناتج عن الحل يجب أن يقترب من الحالة المثالية قدر الإمكان.

4-4 المتطلبات الأمنية في شبكات MANETs:

4-4-1 الموثوقية (Authentication): وتعني إمكانية التحقق من هوية الطرف المتصل بشكل دائم لمنع العقدة المهاجمة من انتحال هوية أحد العقد في الشبكة، ويجب تحقيق هذه الموثوقية في غياب السلطة المركزية في شبكات MANETs.

4-4-2 التوافر (Availability): تعني بقاء الخدمات الموجودة في الشبكة متاحة على الرغم من تعرضها للهجمات التي تحاول إيقاف تلك الخدمات، أي بمعني آخر تعني ضمان استمرارية عمل الشبكة بوجود العقد الخبيثة.

4-4-3 السّرية (Confidentiality): والتي تعني ضمان عدم كشف المعلومات لعقد غير مصرح لها بالاطلاع عليها، وبما أن شبكات MANETs تستخدم قناة اتصال مفتوحة فإن كل العقد التي تقع ضمن مجال الاتصال الراديوي يمكنها الحصول على البيانات وسرقة الاتصال، لذا كان لا بد من تحقيق سرية البيانات من خلال تشفيرها أو استخدام هوائي موجه لتفادي إرسال البيانات في كافة الاتجاهات وخاصة المعلومات الحساسة مثل الاستراتيجيات العسكرية أو أي معلومات عسكرية تكتيكية تتطلب ضمان سريتها وتشفيرها.

4-4-4 عدم التنصل (Non-Repudiation): يُسهل إمكانية تحديد المهاجم بعد حدوث الهجوم، وهذا يمنع أي مهاجم أن يتنصل من هجومه، ولتحقيق هذه الميزة يجب أن تُخزَن كل المعلومات المتعلقة بالعقدة في جدول خاص بها.

4-4-5 الخصوصية (Privacy): تضمن حفظ المعلومات السّرية الخاصة بالعقد مثل الهوية الحقيقية للعقدة، مسار حركتها، السرعة، المفاتيح المستخدمة، بعيداً عن الأشخاص غير المخول لهم الحصول عليها.

4-4-6 التكاملية (Integrity): يجب أن تكون الرسالة محمية من التعديل، أي يجب أن يضمن المرسل وصول الرسالة إلى المستقبل دون أي تعديل، حيث أن أي تعديل في الطرد المرسل يجب أن يتم حصراً من قبل الأشخاص المخولين بذلك.

4-4-7 التحكم بالوصول (Access control): الوصول إلى خدمات معينة يكون محدد محلياً من قبل العقد وذلك وفقاً لسياسات محددة، حيث يُحدَد لكل عقدة تفويض تعمل من خلاله.

5 الفصل الخامس

المحاكاة والنتائج

Simulation and Results

5-1 مقدمة:

وثّقنا في الفصل الأول العديد من الأبحاث والدراسات المرجعية التي درست هجوم الثقب الأسود ضمن شبكات MANETs العاملة مع بروتوكول التوجيه AODV والحلول المُصممة والمُقترحة لتجنب هذا الهجوم، وبما أننا نركز اهتمامنا في هذه الدراسة على استخدام أهم بروتوكولات التوجيه التفاعلية العاملة وفق تقنية Hop-By-Hop، ألا وهو البروتوكول AODV في شبكة MANET، فإن السؤال المطروح الآن ما هي طبيعة الأداء عند استخدام البروتوكول AODV في هذا النوع من الشبكات في ظل وجود هجوم ثقب أسود Black Hole Attack يتم تنفيذه من قبل عقدة أو عدة عقد خبيثة موجودة ضمن الشبكة مشكلة هجوم ثقب أسود بنوعيه الافرادي والتعاوني؟ وكيف يمكن التعديل على هذا الهجوم بحيث يصبح أكثر تعقيداً؟! ويؤثر على شبكة MANET تم افتراض أنها شبكة معادية تعمل بشكل غير مُرخص ضمن بيئة الغير وخارج الحدود الجغرافية للمشغل.

للإجابة على هذه التساؤلات نحتاج إلى وضع نموذج رياضي يعّبر عن كيفية تصّرف العقد المهاجمة لتتمكن من تنفيذ هذا الهجوم ضمن المعطيات البرمجية للبروتوكول AODV، وذلك في حالات مختلفة للشبكة من حيث تغير عدد العقد المهاجمة وتغير كثافة الشبكة في ظل شبكة ديناميكية بحركة عقد بسرعات محددة، ونحتاج أيضاً إلى أن تكون الخوارزمية المُقترَحة لتنفيذ هذا الهجوم مُعدَلة بحيث تصبح أكثر فعالية وأشد تأثيراً.

وسوف نقوم في سياق هذا الفصل بتقييم الدراسات السابقة التي تم شرحها في الفصل الأول من هذا البحث والتي تناولت هذا الهجوم ضمن بيئة تحوي البروتوكول AODV من خلال مناقشة فعالية الحلول المُتبعة ضمنها وذلك بناءً على آلية الهجوم المُقترحة، ويتم ذلك باستخدام محاكي الشبكات NS-2.35 الذي يوفر البيئة اللازمة والمناسبة لتنفيذ هذا العمل.

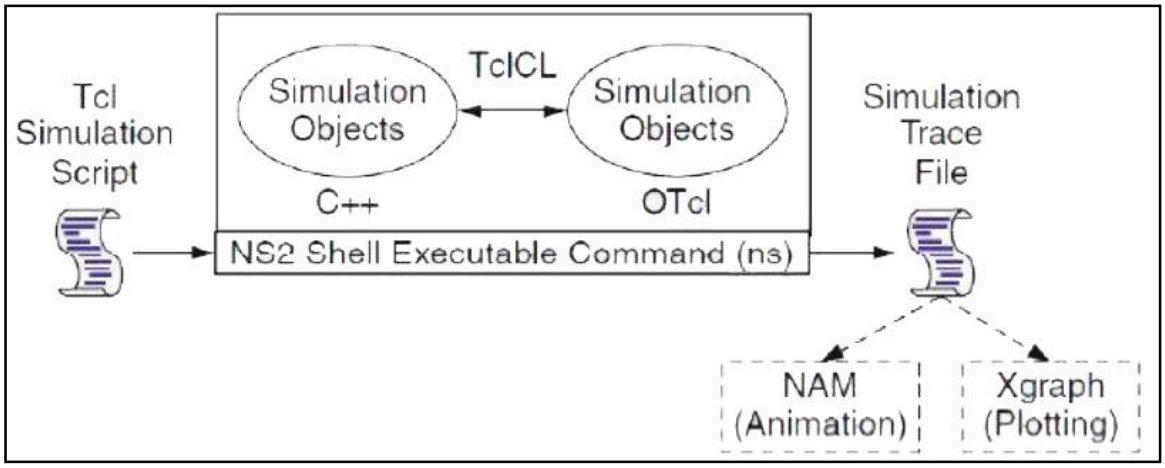
نستهل هذا الفصل في توضيح آلية تنفيذ هجوم الثقب الأسود بنوعية الافرادي والتعاوني مع بروتوكول التوجيه AODV ثم نوضح النموذج المُقترَح لعمل العقد المهاجمة وفق هذا الهجوم، وتعريف بيئة المحاكاة المستخدمة في هذه الدراسة والمتمثلة في المحاكي NS-2.35، حيث نقدم شرحاً لبيئة هذا المحاكي وآلية العمل في هذه البيئة (كيفية إنشاء سيناريوهات المحاكاة واستخلاص النتائج)، وتحديد أداء الشبكة من خلال قياس بارامترات هي الإنتاجية Throughput ومعدل وصول الرزم Packet Delivery Rate (PDR) والتأخير الزمني الكلي (تأخير زمن العبور) End-To-end Delay (ETD).

5-2 محاكي الشبكات NS-2.35:

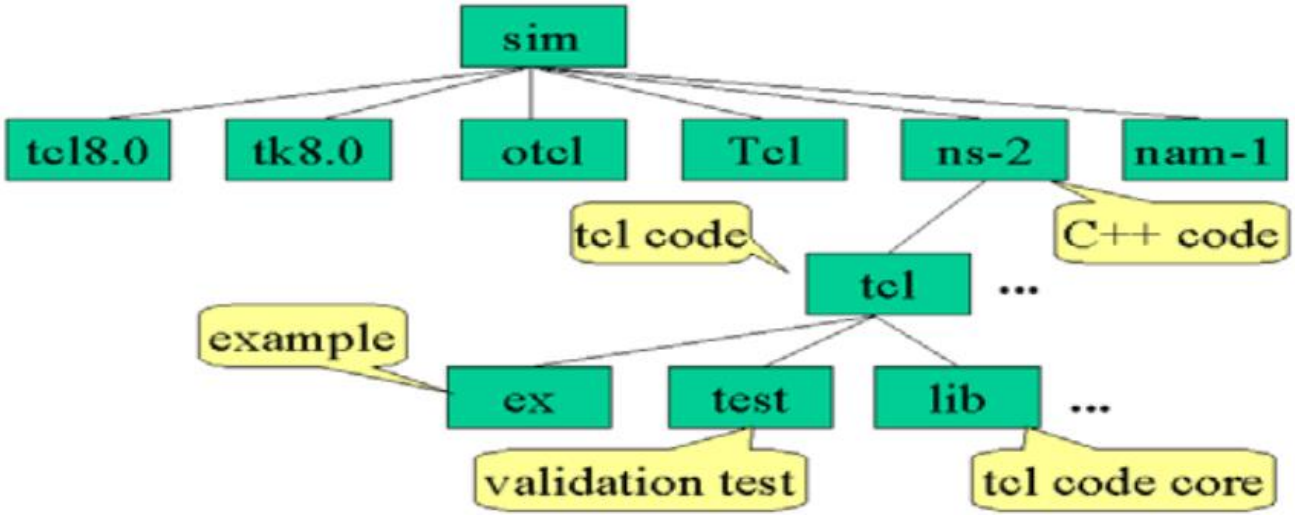
محاكي الشبكات NS-2.35 هو الإصدار الثاني من محاكي الشبكات Network Simulator، تطوير جامعة كاليفورنيا، حيث يستخدم هذا المحاكي لمحاكاة عدد كبير من الشبكات السلكية واللاسلكية، ويعتمد في مبدأ عمله مبدأ محاكاة الأحداث المتقطعة discrete event simulator، وينفذ هذه المحاكاة على مستوى الرزم packet level، ويدعم هذا المحاكي عدد كبير من بروتوكولات التوجيه، ويتم محاكاة الشبكات من خلال كتابة الأوامر النصية في الواجهة Terminal الموضحة بالشكل (5-1).

الشكل (5-1) الواجهة Terminal للمحاكي NS-2.35 في نظام التشغيل Ubuntu

يرتكز هذا المحاكي في عمله على لغتين وهما: لغة C++ التي تستخدم مترجم compiler لترجمة أوامرها، ولغة OTcl التي تستخدم مفسر interpreter لتفسير أوامرها، وتعد لغة C++ قوية وسريعة التنفيذ ولغة OTcl بطيئة لكنها سهلة الاستخدام، يُكتب بلغة C++ كل من مسار البيانات ومعالج الرزم ومولد المحاكاة، ويُكتب بلغة OTcl مسارات التحكم والتهيئة وسيناريو المحاكاة، ويتم استخدام لغة TclCL من أجل عملية الربط بين اللغتين.



الشكل (5-2-A) لغات العمل في محاكي الشبكات NS-2.35



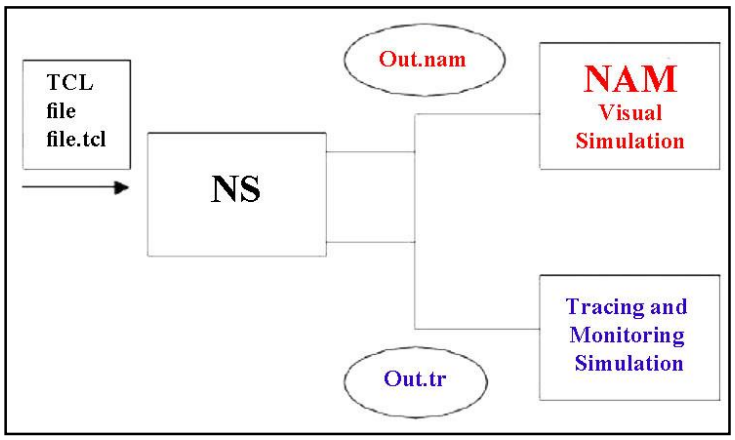
الشكل (5-2-B) هيكلية بناء المحاكي NS-2.35

5-3 عملية المحاكاة باستخدام NS-2.35:

تتضمن عملية المحاكاة باستخدام هذا المحاكي ثلاث خطوات وهي:

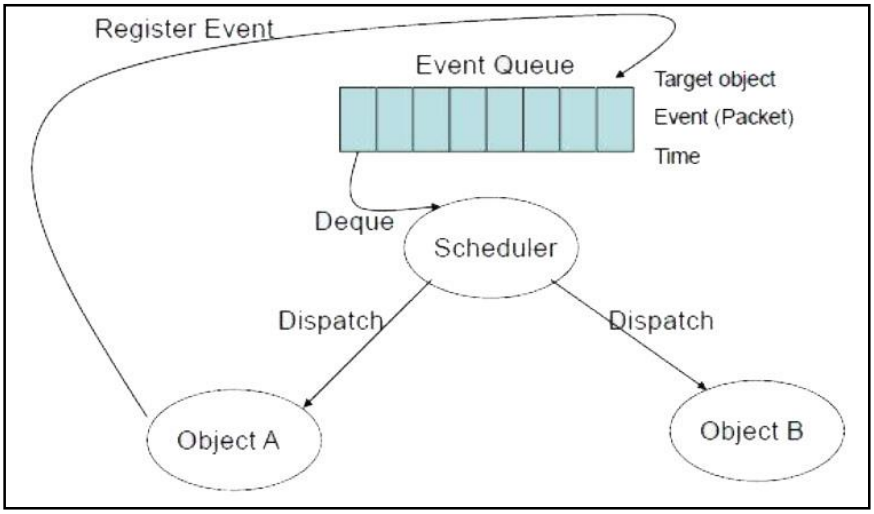
1. تصميم المحاكاة (طريقة المحاكاة والنتائج المتوقعة).
2. التهيئة وتشغيل المحاكاة: وتتضمن تهيئة الشبكة (العقد والوصلات)، تهيئة المحاكاة (الساعات والأحداث)، تشغيل المحاكاة.

3. عملية القياس (نتائج، تحليل)، لإظهار شكل الشبكة وحركة الرزم وتستخدم برنامج NAM حيث يقوم بقراءة ملف الخرج Out.nam، ومن أجل تتبع ومراقبة الرزم يتم قراءة ملف الخرج Out.tr، أما لإظهار النتائج بشكل مخططات نستخدم برنامج XGRAPH.



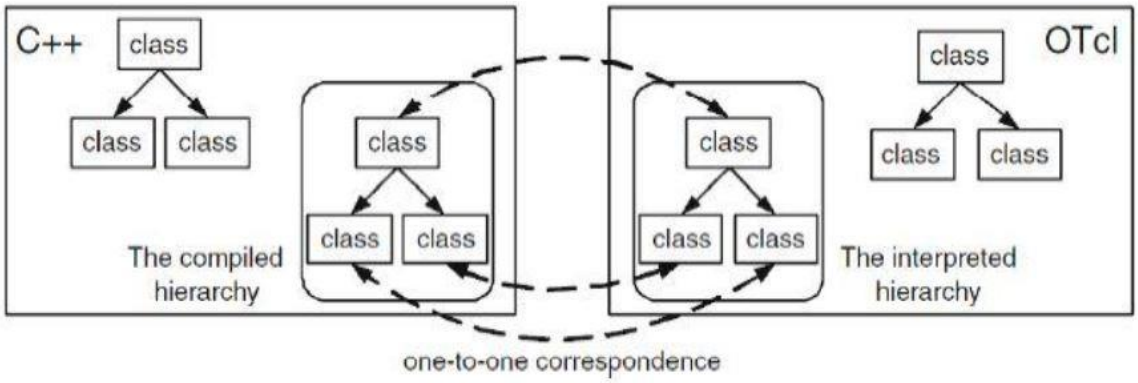
الشكل (5-3) عملية المحاكاة باستخدام NS-2.35

- وبما أن البرنامج يعتمد مبدأ محاكاة الأحداث المتقطعة يتم ترتيب الأحداث زمنياً ويُعطى لكل حدث رقم معرف ID، ويقوم المجدول بجدولة الأحداث وترتيبها حيث تتم معالجة الحدث عند وقوعه والإجراء الذي يقوم بمعالجة الأحداث يسمى Handler.



الشكل (5-4) جدولة الأحداث في المحاكي NS-2.35

- يتضمن المحاكي مجموعة من الأصناف Classes ترتبط مع بعضها البعض وتؤمن الربط بين اللغتين، وتتوضع هذه الأصناف بشكل هرمي ضمن مستويين هما: أصناف لغة C++ وتعتمد مبدأ الترجمة، وأصناف لغة OTcl وتعتمد مبدأ التفسير، علماً أن العلاقة بين هذه الأصناف هي علاقة صنف لصنف One-to-One.



الشكل (5-5) توزع الأصناف في لغتي C++ و OTcl

- الصنف Simulator هو الصنف الأساسي في البرنامج حيث يقوم بعملية المحاكاة، ويحتوي مجموعة من الواجهات interfaces تقوم بتهيئة عملية المحاكاة واختيار نوع المجدول المناسب.
- باستخدام لغة OTcl لدينا نمطين من أنماط العمل وهما: نمط العمل التفاعلي Interactive mode وفيه تتم عملية الكتابة على الواجهة Terminal بشكل مباشر، ونمط الدفعة الواحدة Batch mode وفيه يتم العمل من خلال إنشاء ملفات تكتب بلغة OTcl وتُحفظ بصيغة tcl وبعد ذلك من أجل تنفيذ البرنامج نستدعي الملف المحفوظ كما يلي: ns file_name.tcl في الواجهة terminal.

5-4 خطوات كتابة برنامج باستخدام NS-2.35:

إن عملية كتابة برنامج بلغة OTcl باستخدام المحاكي NS-2.35 هي عملية منظمة تتم وفق المراحل التالية:

1. إنشاء مجدول الأحداث Create the event scheduler.
2. تفعيل عملية التعقب setup tracing operation.
3. بناء طوبولوجيا الشبكة Create network topology.
4. تعريف نماذج للأخطاء Insert error modules.
5. تعريف وكيل الاتصال (transport) Create connection.
6. تعريف التطبيق المستخدم (application) Create traffic.
7. جدولة الأحداث Schedule events
8. بدء عملية المحاكاة Start the Simulation.

5-5 هجوم الثقب الأسود مع البروتوكول AODV:

بما أن البروتوكول AODV يعتمد في عملية اكتشاف المسار على شعاع المسافة Distance Vector، بحيث يفترض أن المسار الأمثل المتوفر باتجاه الهدف هو المسار ذو عدد القفزات hop-counts الأقل والذي يحقق أقل تكلفة ممكنة لتبادل البيانات بين المصدر والهدف، لذلك فإن المهاجم بهجوم الثقب الأسود يعتمد على هذه الثغرة لتنفيذ هجومه على الشبكة العاملة وفق هذا البروتوكول، علماً أنه يوجد شكلين لتنفيذ هذا الهجوم فيمكن فإما أن يُنفَذ من قبل عقدة خبيثة واحدة ويسمى هجوم ثقب أسود فردي Single Black Hole Attack، أو يُنفذ من قبل عدة عقد خبيثة تعمل معاً بأحد الأشكال التعاونية ويسمى عندها هجوم ثقب أسود تعاوني Cooperative Black Hole Attack، ويتم شن هذا الهجوم كما يلي:

- عندما تريد العقدة المصدر Source Node العاملة مع البروتوكول التفاعلي AODV إرسال بيانات إلى عقدة أخرى ضمن الشبكة هي العقدة الهدف Destination Node فإنها تقوم بتفعيل عملية بحث عن مسار لهذا الهدف وذلك من خلال إرسال رسالة طلب مسار Route Request (RREQ) على شكل بث عام Broadcast إلى كل جيرانها.

- تقوم العقدة الخبيثة Malicious Node الموجودة ضمن الشبكة والعاملة وفق خوارزمية توجيه تعتمد على كل خصائص البروتوكول AODV بالإضافة إلى خصائص هجومية أخرى وفق هجوم الثقب الأسود Black Hole Attack بالتعامل مع رسالة طلب المسار من خلال إرسال رسالة إجابة Route Reply وهمية للمرسل بشكل مباشر دون إجراء عملية بحث ضمن جدول توجيهها عن مسار متاح لهذا الهدف، بحيث تملك هذه الرسالة نفس بنية رسالة الإجابة RREP الحقيقية للبروتوكول AODV، تظهر العقد الخبيثة من خلال هذه الرسالة بأنها تملك أفضل مسار متاح باتجاه الهدف بأقل تكلفة ممكنة بأقل عدد قفزات بحيث hop-count = 1، وأعلى رقم تسلسلي Sequence Number (SN)، وذلك من خلال عملية مراقبة مُسبقة وبشكل دوري لتغير الأرقام التسلسلية في الشبكة لمعرفة أعلى رقم تسلسلي موجود والذي يدل على المسار الأحدث للهدف.

- عندما يستلم المرسل رسالة الإجابة RREP يطلع على محتوها فيجد أنها تحوي أفضل مسار ممكن للهدف، وبالتالي سوف يقوم بإرسال البيانات عبر المسار المُحدد من قبل العقدة الخبيثة.

- بعد ذلك تصل البيانات المُرسَلة إلى العقدة الخبيثة ولا تقوم بتوجيهها بل تقوم إما بحذفها مباشرة أو خلق حلقات توجيه وازدحام في الشبكة في حال وجود عدة عقد خبيثة تعمل معاً.

5-6 تقييم الدراسات السابقة:

تناولت العديد من الدراسات المرجعية التي تم ذكرها في الفصل الأول هجوم الثقب الأسود مع البروتوكول AODV وتم في هذه الدراسات اقتراح العديد من الحلول لتفادي هذا الهجوم وفق العديد من الطرق والتقنيات، لكن معظم هذه الحلول كانت حلول لحالات فردية وخاصة للهجوم ضمن شروط وظروف عمل محددة جداً لعمل الشبكة بحيث تصبح هذه الحلول غير مفيدة في ظل النموذج المُقترح في هذا البحث لشن هجوم الثقب الأسود، بحيث إن تلك الحلول إما عالجت فقط مشكلة هجوم الثقب الأسود الفردي Single Black Hole Attack بعقدة خبيثة واحدة فقط، أو سببت الحلول المقترحة زيادةً كبيرة في التأخير الزمني ضمن الشبكة، ونتج عن بعضها حمل توجيه Overhead عالة جداً وفي بعض الحالات أكثر من ضعف حمل التوجيه الطبيعي ضمن الشبكة، أو عالجت هجوم الثقب التعاوني بشكل مُقتصر على شروط دقيقة جداً وحالات خاصة لعمل الشبكة، على سبيل المثال عقدتين مهاجمتين فقط، أو افترضت بعض الحلول كشف العقد المهاجمة من خلال حساب معدل التوجيه لكل عقدة من عقد الشبكة وذلك من خلال إيجاد النسبة النسبة التالية: $\left[\frac{\text{عدد الرزم المستقبلة}}{\text{عدد الرزم المرسلة}}\right]$ ، وبالتالي يصبح هذا النوع من الحلول غير مجدي وفق خوارزمية الهجوم المقترحة في هذا البحث، وافترض أحد الحلول عدم وجود حركية في الشبكة أي أن العقد ثابتة وبالتالي يصبح هذا الحل غير مجدي في حال شبكة ديناميكية تحوي حركية للعقد. وتم تصنيف هذه السلبيات لكل دراسة ضمن الجدول التالي:

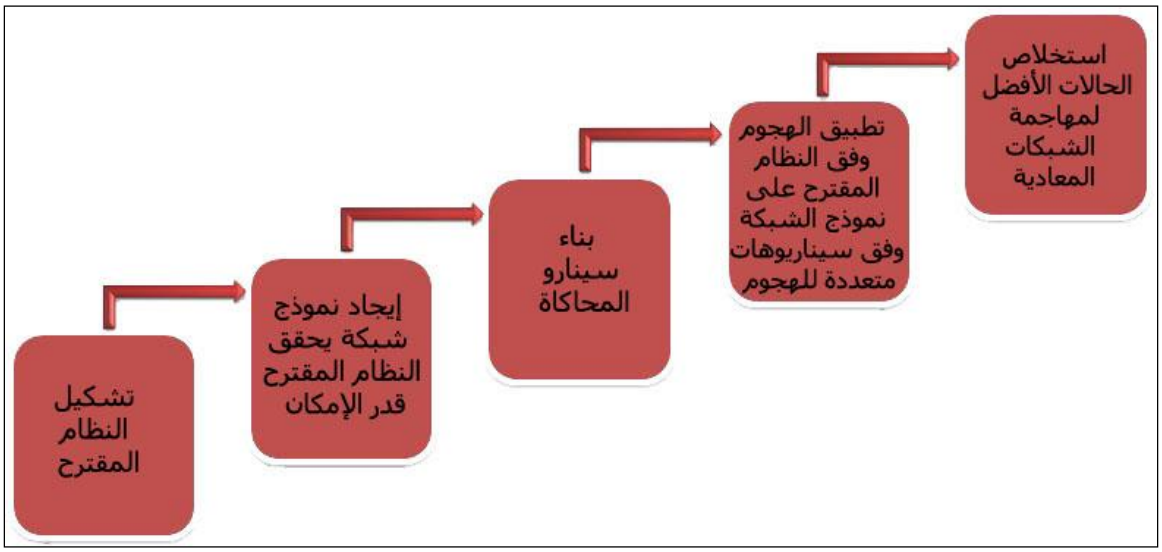
اسم الدراسة	تاريخها	اسم الباحث	عيوبها
Secure Routing to Avoid Black Hole Affected Routes in MANET [3]	2016	Deshmukh, S. R, & Chatur, P. N.	لم يتم تنفيذ الحل حيث بقيت حلاً مقترحاً
Cluster-based Technique for Detection and Prevention of Black-Hole Attack in MANETS [8]	2017	Saurabh, V. K., Sharma, R., Itare, R., & Singh, U	الحل المقترح يسبب تأخير زمني كبير لم يتم قياسه وتعالج مشكلة هجوم الثقب الأسود الفردي فقط
Hybrid Detection of Black hole and Gray hole attacks in MANET [4]	2016	Rathiga, P., & Sathappan, S.	تعالج مشكلة هجوم الثقب الأسود الفردي فقط

الحل المقترح لم يتم تنفيذه، وتسبب تكلفة إضافية بشكل دائم وغير مقبولة وتأخير زمني	Khattak, H.	2013	A Hybrid Approach for Preventing Black and Gray Hole Attacks in MANET [2]
ينتج عنها زيادة كبيرة في التأخير الزمني	Dhende, S., Musale, S., Shirbahadurkar, S., & Najan, A.	2017	SAODV: Black Hole and Gray Hole Attack Detection Protocol in MANETs [9]
تنخفض فعالية الحل المقترح عند زيادة عدد العقد المهاجمة في الشبكة	Sharma, N., & Bisen, A. S.	2016	Detection As Well As Removal Of Black hole And Gray hole Attack In MANET [5]
يبقى معدل نقل البيانات في الشبكة أقل من معدل الحالة الطبيعية للبروتوكول	Nitnaware, D., & Thakur, A.	2016	Black Hole Attack Detection and Prevention Strategy in DYMO for MANET [7]
يبقى إداء الحل المقترح أقل من الحال الطبيعية بكثير حيث تسبب تحسبن طفيف جداً في أداء الشبكة وأيضاً من أجل عدد عقد مهاجمة لا تزيد عن عقدتين	Gurung, S., & Saluja, K.	2014	Mitigating Impact of Black hole Attack in MANET [34]
الحل المقترح يعالج مشكلة هجوم الثقب الأسود الفردي فقط وتسبب زيادة كبيرة في حمل التوجيه وتأخير زمني كبير	Gurung, S., & Chauhan, S.	2019	A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET [11]

الجدول (5-1) تقييم الدراسات السابقة

5-7 منهجية البحث:

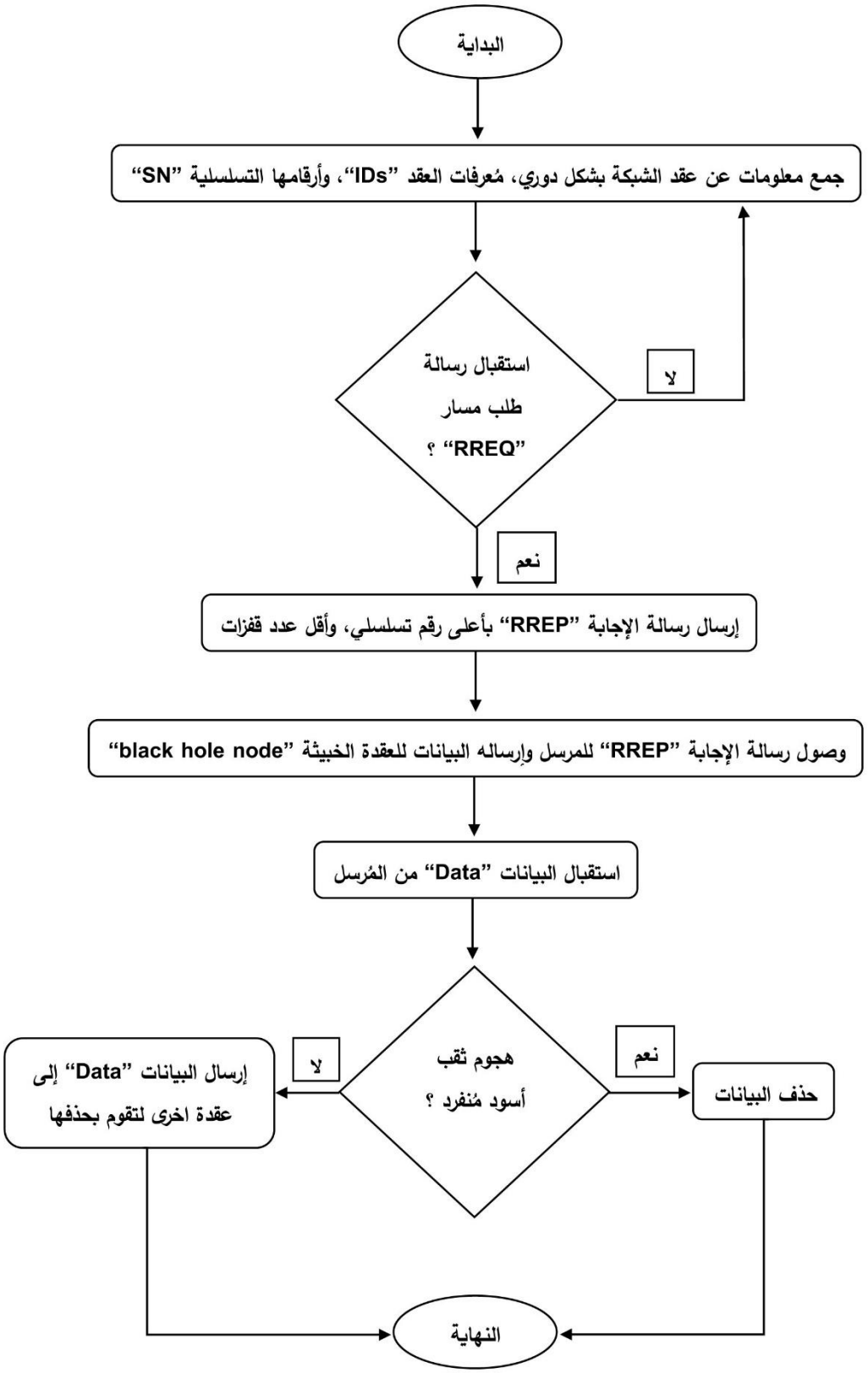
تتلخص منهجية البحث اعتماداً على الدراسات السابقة في تنفيذ العديد من الخطوات الرئيسية التي تبدأ بتطبيق خوارزمية عمل للعقد المهاجمة لتنفيذ هجوم ثقب أسود إفرادي أو تعاوني مكون من عدة عقد خبيثة تشترك في تنفيذ الهجوم بهدف تعطيل شبكة MANET معادية والتأثير على تبادل البيانات ضمنها ومحاولة حجبه بشكل كامل، وبعد ذلك يتم تطبيق الهجوم المقترح ضمن شبكة MANET تعمل بعض العقد ضمنها وفق البروتوكول AODV المُعدل والذي تمت تسميته BAODV، بحيث تكون العقد الخبيثة العاملة وفق هذا البروتوكول قادرة على التواصل مع عقد الشبكة الأخرى العاملة وفق البروتوكول AODV الطبيعي والمشاركة في تبادل الرسائل معها، ثم ننتقل في الخطوة التالية إلى تطبيق عدة سيناريوهات لتنفيذ الهجوم متباينة من حيث عدد العقد المهاجمة وكثافة الشبكة العاملة ومواقع هذه العقد، ونصل في النهاية الى تقييم أداء الشبكة في ظل تأثير هذا الهجوم وذلك من خلال مراقبة العديد من بارامترات الأداء الأساسية المحددة لفعالية تنفيذ الهجوم، ويوضح الشكل (5-6) هذه المراحل لإنجاز العمل.



الشكل (5-6) مراحل العمل

5-7-1 تشكيل النظام المقترح:

تم تعديل خوارزمية العمل للعقد المهاجمة بحيث تنفيذ هجوم الثقب الأسود وفق شبكة عاملة مع بروتوكول التوجيه AODV ونتج لدينا عقد تعمل وفق البروتوكول BAODV وفق المخطط الصندوقي التالي:



الشكل (5-7) المخطط الصندوقي لعمل العقدة الخبيثة وفق البروتوكول BAODV

تم تطبيق الخوارزمية المُقترحة لعمل العقدة الخبيثة من خلال التعديل على البنية البرمجية للبروتوكول AODV المكتوبة بلغة C++، وذلك بتعديل الملفين البرمجيين aodv.cc وَ aodv.h، بحيث تم تضمين الخوارزمية في الملف aodv.cc وتم التصريح عن العقد المهاجمة في الملف aodv.h.

يوضح المخطط الصندوقي خوارزمية العمل للعقدة المهاجمة حيث إنه عند بداية عمل الشبكة بدءً من اللحظة الزمنية 0.0 ثانية تقوم العقدة الخبيثة بتبادل رسائل الترحيب HELLO_messages مع عقد الشبكة الأخرى المجاورة لها والتي تُرسل على شكل بث عام broadcast لكل الجوار وبشكل دوري خلال فترات زمنية محددة بالميلي ثانية: HELLO_INTERVAL=1، وتتضمن هذه الرسائل الرقم التسلسلي SN وعدد القفزات HOP_COUNT ولها فترة صلاحية هي زمن الحياة TTL لهذه الرسائل، وهذه الصلاحية محددة بمعاملين وهما: الفاصل الزمني لإرسال رسائل الترحيب وهو HELLO_INTERVAL والعدد الأعظمي المسموح للضياعات وهو ALLOWED_HELLO_LOSS، بحيث يُعطى زمن الحياة وفق الجداء ALLOWED_HELLO_LOSS*HELLO_INTERVAL، وبالتالي من خلال هذه الرسائل تتمكن العقدة الخبيثة من معرفة التحديثات الدورية لحالة الشبكة من خلال معرفتها بمعرفات العقد IDs وآخر تحديثات الأرقام التسلسلية لها Sequence Numbers.

تستمر العقدة الخبيثة بجمع المعلومات عن الشبكة وعند تلقيها لأي رسالة طلب مسار Route Request (RREQ) من أي عقدة من عقد الشبكة تتعامل مباشرة مع هذا الطلب دون أي عملية بحث في جدول توجيهها لمعرفة إمكانية امتلاكها مساراً متاحاً للهدف أم لا، وذلك من خلال المبادرة بإرسال رسالة الإجابة Route Reply (RREP) بطريقة بث أحادي unicast إلى العقدة المصدر Source Node (SN) عبر العقدة الوسيطة Intermediate Node التي تلقت منها رسالة الطلب في حال وجودها أو بطريقة مباشرة للعقدة المصدر نفسها في حال كانت على اتصال مباشر معها، وتتميز هذه الرسالة بتكلفة مسار منخفضة جداً، حين إن العقدة الخبيثة تؤمن المسار المثالي نحو الهدف من خلال إرسال رسالة إجابة برقم تسلسلي هو الأعلى وعدد قفزات أقل ما يمكن (يساوي 1) كما يوضح الأسطر البرمجية التالية من ملف aodv.cc:

```
else if(index==malicious1) { seqno = max(seqno, rq->rq_dst_seqno)+1;

sendReply(rq->rq_src,          // IP Destination

1);                  // Hop Count
```

بعد ذلك تصل رسالة الإجابة من العقدة الخبيثة إلى المرسل، وتصل أيضاً العديد من رسائل الإجابة من عقد أخرى تملك مسار نحو الهدف في الشبكة، وبناءً على رسالة العقدة الخبيثة سوف يجد المرسل الذي يعمل وفق البروتوكول AODV والذي يعتمد مبدأ شعاع المسافة Distance Vector الأقصر في اختيار المسار الأفضل أن أقصر مسار متوفر هو المسار المُقدَم من العقدة الخبيثة، وفي حال تساوي مسارين في عدد القفزات فإن الرقم التسلسلي للهدف في رسالة الإجابة القادمة من العقدة الخبيثة سيكون الأعلى، أي أنها تملك المسار الأحدث للهدف.

وبناءً على ذلك سوف يقوم المرسل بتوجيه البيانات إلى العقدة الخبيثة، وعندما تصل البيانات إلى العقدة الخبيثة سوف تقوم بإسقاطها مباشرة في حال كانت تعمل بشكل فردي (Single Black Hole Attack)، أو تقوم بتوجيهها إلى عقدة خبيثة أخرى لصنع حلقات في الشبكة، بحيث تقوم العقدة الثانية بحذفها مشكلة هجوم ثقب تعاوني (Cooperative Black Hole Attack)، كما توضح الأسطر التالية:

```
if(strcmp(argv[1], "blackhole1") == 0) {
malicious1= index;
printf("malicious %d", malicious1);
return TCL_OK;
   }
drop(p, DROP_RTR_NO_ROUTE);

else if((index==malicious2)|| (index==malicious3));
sendError(rerr, false);
```

5-7-2 نموذج الشبكة:

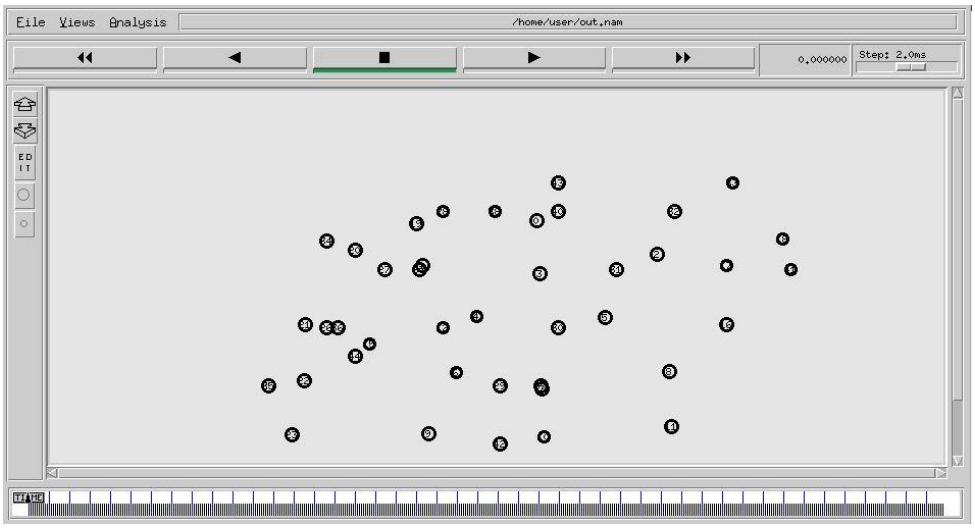
بعد تعديل البنية البرمجية للبروتوكول AODV وإنتاج الخوارزمية المُعدلة BAODV المحددة لعمل العقد المهاجمة أصبحنا قادرين على كتابة ملف الشبكة العاملة بلغة TCL وفق بروتوكول التوجيه BAODV بحيث نصرح عن العقد الخبيثة بلغة TCL بالصيغة التالية:

```
$ns at 0.0 "[$n6 set ragent_] hacker"
```

على سبيل المثال يدل هذا السطر على أن العقدة 6 تسلك سلوك عقدة مهاجمة عند بداية عمل الشبكة في اللحظة الزمنية 0.0 ثانية.

حيث تم تعريف شبكة MANET تعمل وفق معيار الاتصال IEEE 802.11b ذات كثافة متغيرة بعقدة مهاجمة واحدة فقط أو عدة عقد مهاجمة.

تُمثِل الشبكة المدروسة مجموعة من أجهزة الحاسب التي تشكل شبكة "MANET" بدون بنية تحتية، تم تحديد تموضع العقد بشكل مُحدد، وبعض العقد تتحرك وفق مسارات محددة ضمن حدود الشبكة، كما هو موضح في الشكل(5-8).



الشكل (5–8) شبكة بحجم 45 عقدة

تم تشغيل المحاكاة لمدة 100 sec بمساحة شبكة تبلغ 584m * 1186m وتوضع عقد بدائي عشوائي، حيث تم إنشاء عدة سيناريوهات لدراسة أداء البروتوكول في حالة الشبكات الصغيرة والمتوسطة والكبيرة وبحركية للعقد حيث كانت العقد تتحرك بسرعة 40 m/sec، تم اختيار تطبيق نقل ملفات بحجم 2 Mb من أجل تحقيق حمل كبير ضمن الشبكة، ويبين الجدول التالي البارامترات المستخدمة في المحاكاة:

Simulation Properties	Values
Antenna Model	Omni Antenna
Radio Propagation	Two Ray Ground
Node Distribution	Random
MAC Type	IEEE 802.11 (2.4 GHZ)
Band width	11Mbps
Application Traffic	CBR
Topology	1186 X 584
Channel Type	Wireless Channel
No of Mobile Nodes	15 – 25 – 35 – 45 -55
CBR Packet Size	1500 Byte
Routing Protocol	AODV
Time Of Simulation	100 Seconds
NS Version	NS – all-in-one – 2.35
Traffic Pattern	CBR Sessions
Pause Time	1 second
No Of Black hole Nodes	0 – 1 – 2 – 3 – 4 – 5
Maximum Speed Of Nodes	40 m/sec

الجدول (5–2) بارامترات المحاكاة

5-7-3 مقاييس الأداء:

هناك أنواع عديدة من البارامترات لتقييم أداء بروتوكولات التوجيه، والتي تملك كل منها سلوك مختلف في قياس أداء الشبكة الإجمالي، وفي هذا البحث نتطرق إلى ثلاث بارامترات لمقارنة أداء الشبكة بالنسبة للبروتوكول المدروس AODV في ظل وجود هجوم الثقب الأسود Black Hole Attack، وهذه البارامترات هي: الإنتاجية Throughput، والتأخير الزمني الكلي End-To-end Delay (ETD)، ومعدل وصول الرزم Packet Delivery Rate (PDR).

الإنتاجية Throughput:

تُعرَف الإنتاجية بأنها نسبة البيانات الإجمالية التي يتم استقبالها من المُرسل، وترتبط الإنتاجية بالزمن المستغرق من قبل المستقبل لاستقبال الرسالة الأخيرة، وتقاس بالبايت أو البت بالثانية (Bytes/sec, bits/sec)، وتُعطى الإنتاجية بالعلاقة التالية:

$$Throughput = \frac{size\ of\ correctly\ received\ data(Bytes/bits)}{time\ (s)}$$

وهناك العديد من العوامل التي تؤثر على الإنتاجية، ومثال ذلك:

- التغيرات العديدة في طوبولوجيا الشبكة.
- الاتصال غير الموثوق بين العقد.
- عرض الحزمة المتوفر المحدود.
- الطاقة المحدودة.

التأخير الزمني الكلي End-To-end Delay (ETD):

التأخير الزمني نهاية إلى نهاية هو الزمن المستغرق من لحظة توليد الرزمة من قبل المصدر وحتى استقبالها من قبل الوجهة، وبالتالي هو الزمن الذي تستغرقه الرزمة حتى تعبر الشبكة ويُقاس بالثانية أو بالميلي ثانية، وبعض التطبيقات حساسة جداً لتأخير الرزمة مثل الصوت الذي يُعد تطبيق حساس جداً للتأخير، أي أن التأخير الزمني الكلي يمثل متوسط الزمني لوصول الرزم بنجاح إلى وجهتها النهائية، ويعطى بالعلاقة التالية:

$$ETD = \frac{\sum_{i=1}^{nodes} \left[arrival\_time\ (p)\ \_\ send\_time(p)\ \right]}{Number\ of\ Connections}$$

ولدينا أنواع عديدة من التأخيرات وهي:

- تأخير المعالجة Processing Delay (PD).
- تأخير النسق Queuing Delay (QD).
- تأخير الإرسال Transmission Delay (TD).
- تأخير الانتشار Propagation Delay (PD).

معدل وصول الرزم Packet Delivery Rate (PDR):

يعّبر معدل وصول الرزم عن نسبة مجموع كل الرزم المُستقبلة في الشبكة من قبل كل العقد إلى الرزم المُرسلة في الشبكة من قبل كل العقد، ويُحسب هذا البارامتر كنسبة مئوية، ويُعطى بالعلاقة التالية:

$$PDR = \frac{\sum_{i=1}^{nodes} packets\_received}{\sum_{i=1}^{nodes} packets\_sent} * 100\%$$

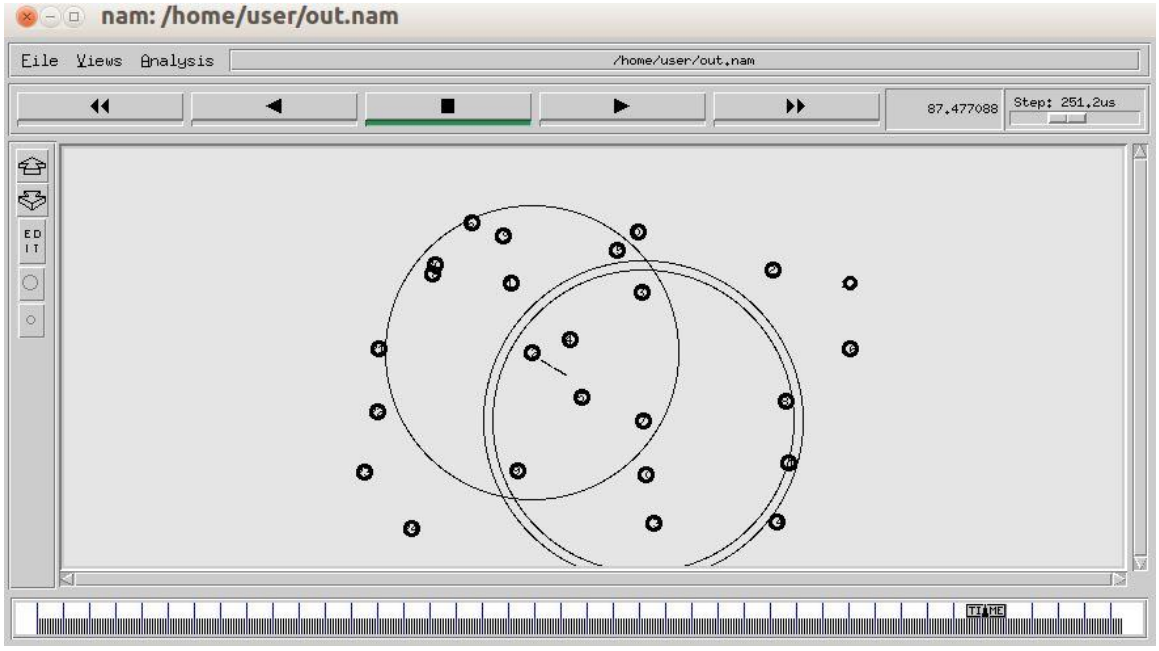
5-7-4 سيناريوهات المحاكاة:

لقد قمنا بدراسة حالة الشبكة ضمن ثلاث سيناريوهات حيث كان السيناريو الأول يقارن بين حالتي عدم وجود هجوم ووجود هجوم بعقدة خبيثة واحده فقط ثم عقدتين وذلك لشبكة بكثافة متوسطة مؤلفة من 25 عقدة، أما في السيناريو الثاني فقد قمنا بتطبيق هجوم ثقب أسود تعاوني مكون من 4 عقد مهاجمة تعمل معاً وذلك في شبكة ذات كثافة عقد متغيرة 55 – 45 – 35 – 25 – 15 عقدة، وفي السيناريو الثالث تم تطبيق هجوم ثقب أسود تعاوني أيضاً ولكن بعدد عقد خبيثة متزايد 0 – 1 – 2 – 3 – 4 – 5 عقدة، وذلك تحت كثافة ثابتة للشبكة (35 عقدة)، علماً أنه في السيناريو الأول تم قياس الإنتاجية أما في السيناريوهين الثاني والثالث تم الانتقال لقياس متوسط الإنتاجية للحصول على توصيف أكثر دقة لسلوك البروتوكولAODV في ظل وجود الهجوم وذلك كما يلي:

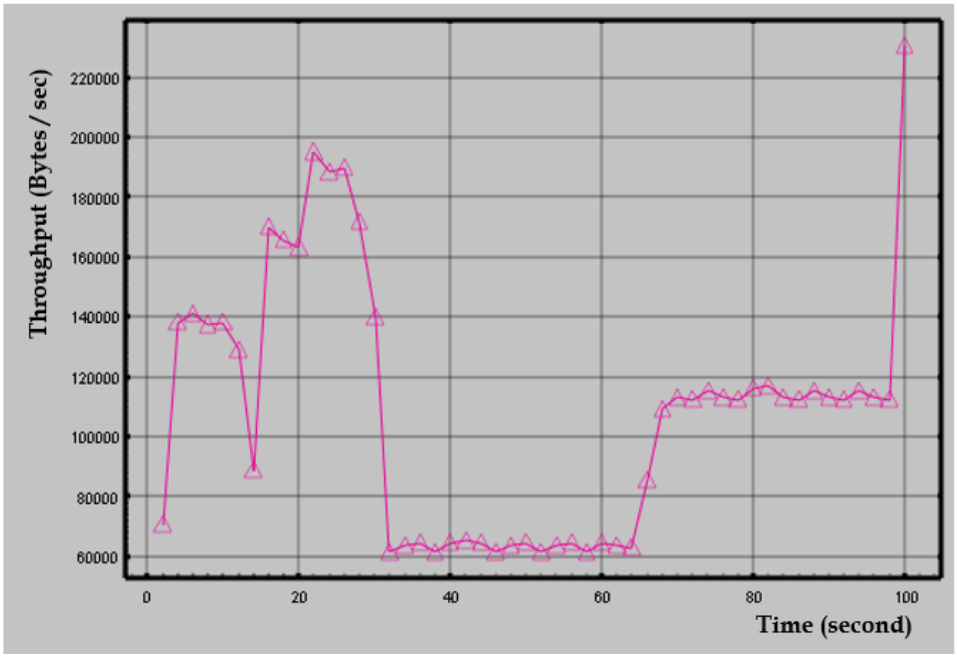
الشكل (5-9) سيناريوهات المحاكاة

السيناريو الأول:

A. شبكة مؤلفة من 25 عقدة، ومدة المحاكاة 100 sec، ولا توجد أي عقدة خبيثة كما يلي:

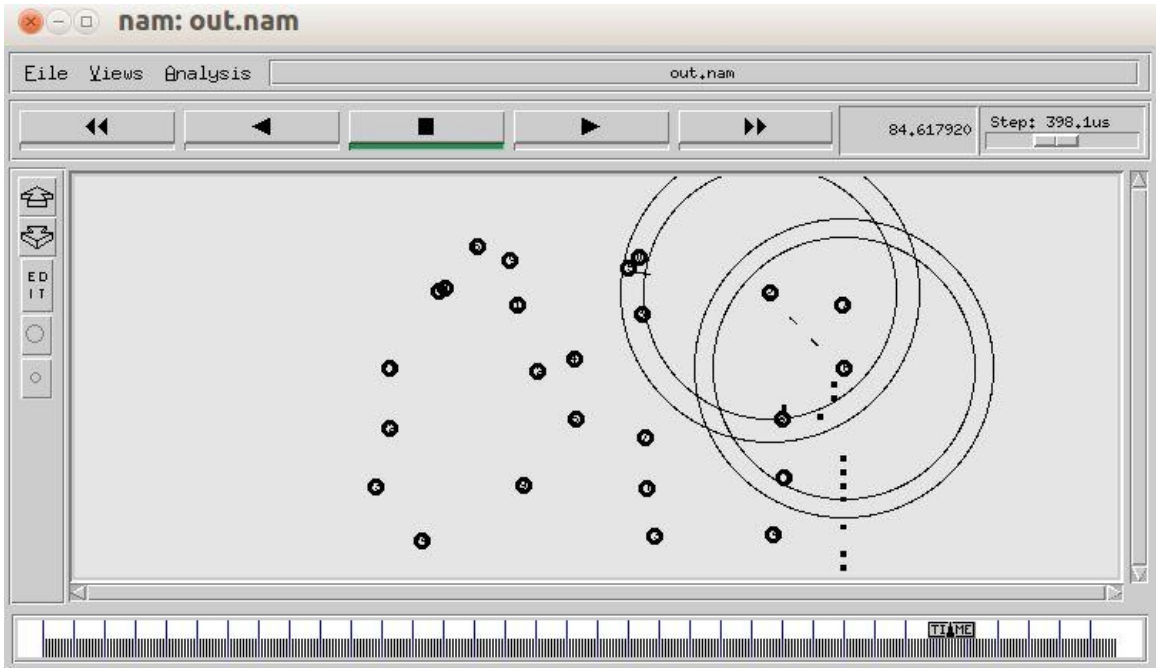


الشكل (5-10) خرج برنامج NAM لشبكة بكثافة 25 عقدة، بدون هجوم

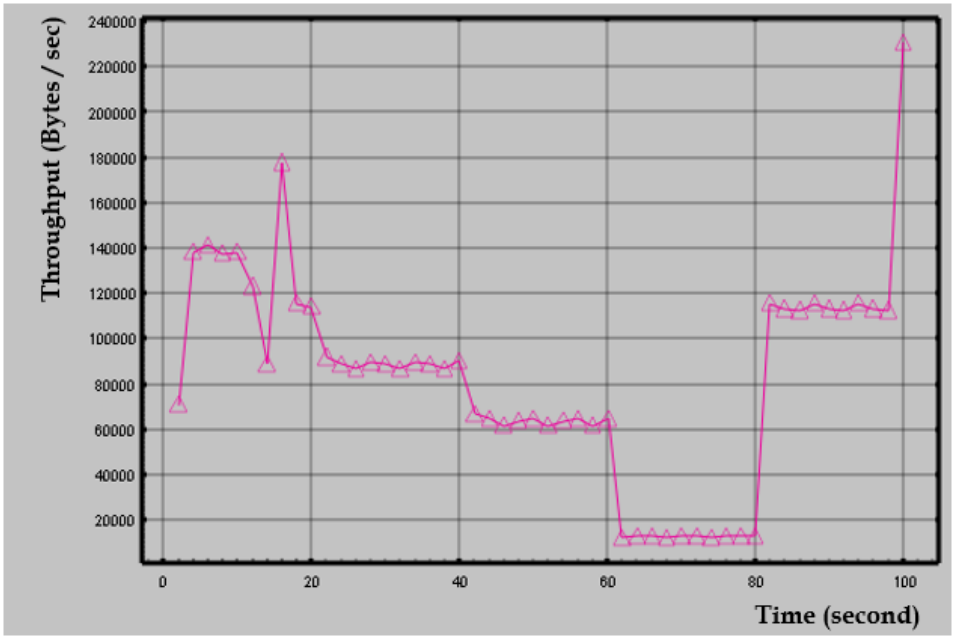


الشكل(5-11) الإنتاجية دون وجود هجوم

B. شبكة مؤلفة من 25 عقدة، ومدة المحاكاة 100 sec، وعقدة خبيثة واحدة فقط كما يلي:

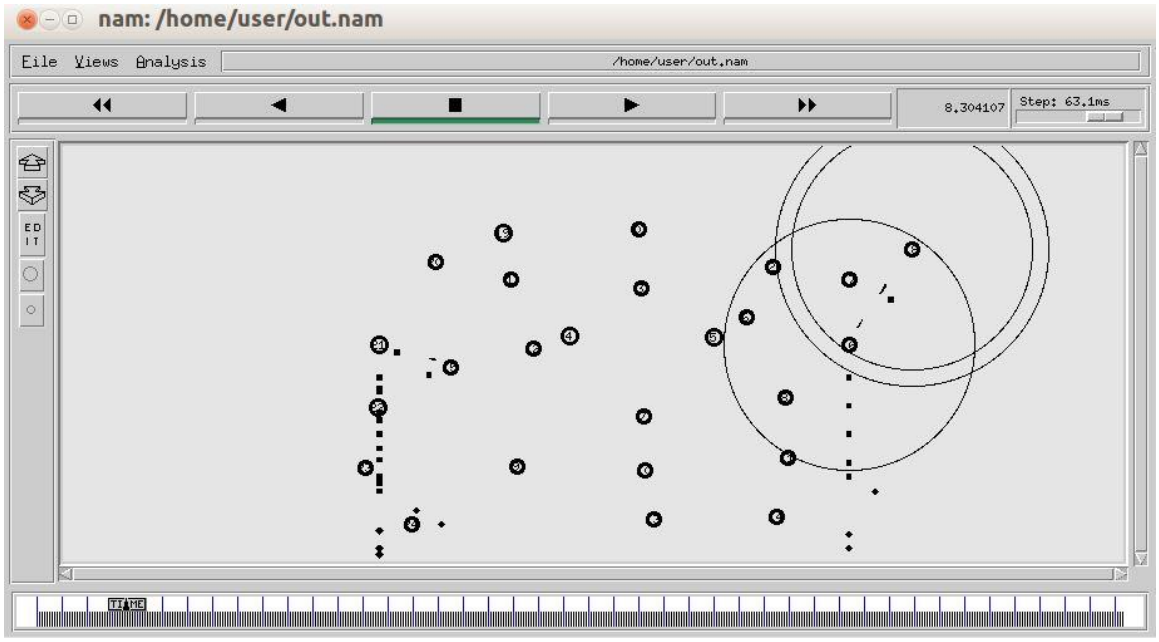


الشكل (5-12) خرج برنامج NAM لشبكة بكثافة 25 عقدة، وهجوم بعقدة خبيثة

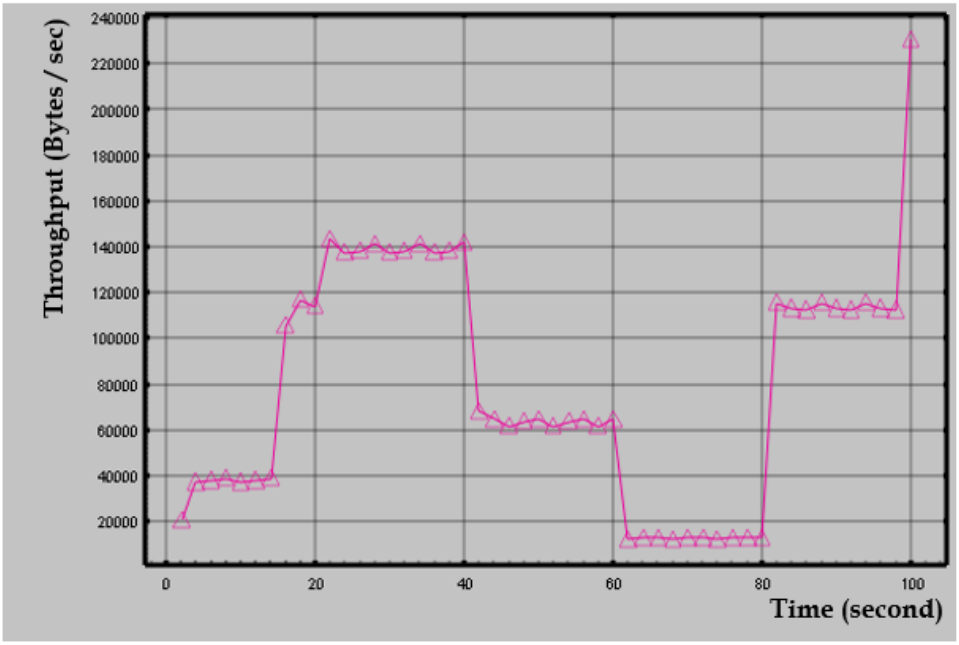


الشكل(5-13) الإنتاجية مع وجود هجوم بعقدة خبيثة واحدة

C. شبكة مؤلفة من 25 عقدة، ومدة المحاكاة 100 sec، وعقدتين خبيثتين كما يلي:



الشكل (5-14) خرج برنامج NAM لشبكة بكثافة 25 عقدة، وهجوم بعقدتين خبيثتين

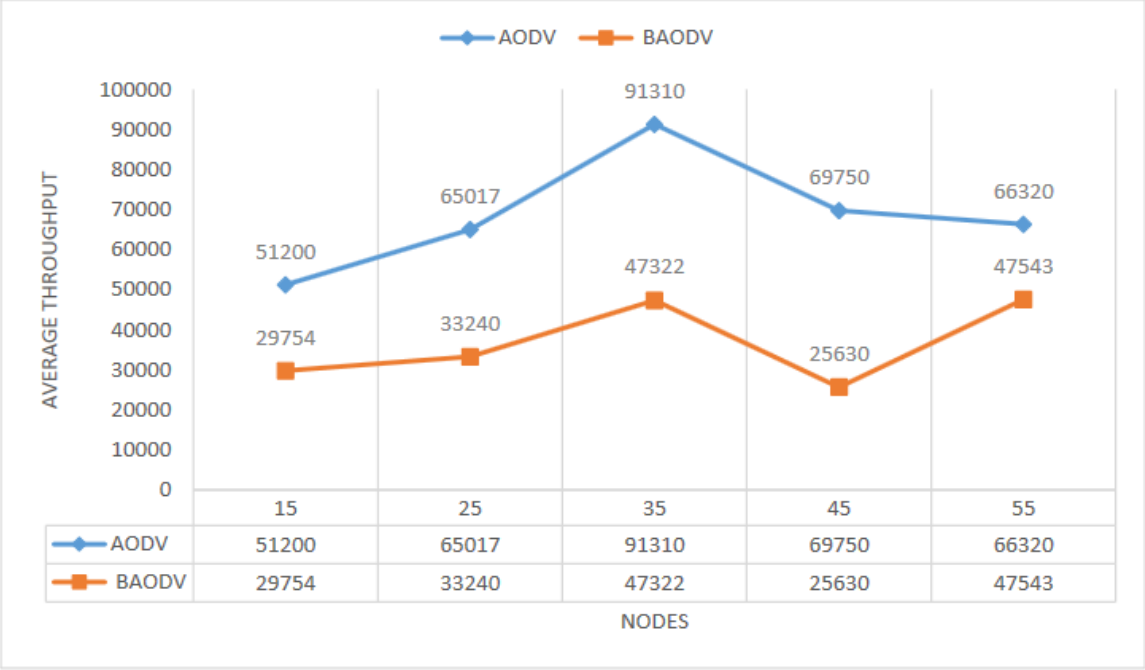


الشكل(5-15) الإنتاجية مع وجود هجوم بعقدتين خبيثتين

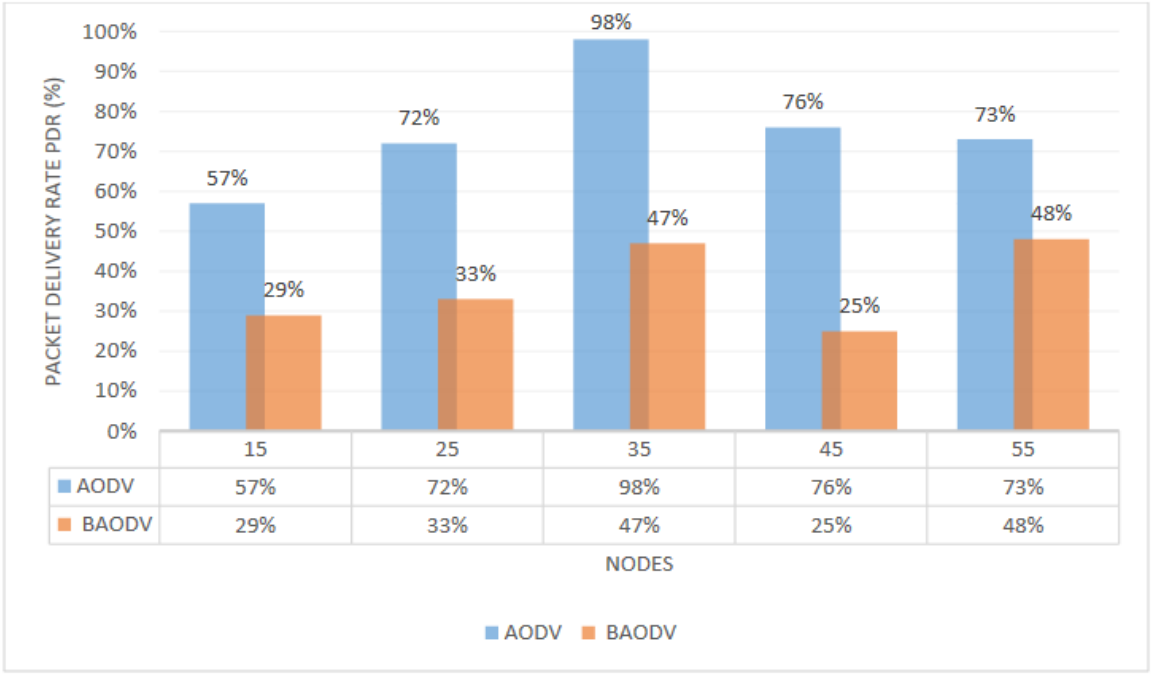
تبين لدينا في السيناريو الأول وبالمقارنة بين الحالتين A و B من خلال النتائج في الشكلين (5-11) و(5-13) حدوث انخفاض في الإنتاجية بالمجمل على طول فترة المحاكاة عند تطبيق الهجوم بعقدة خبيثة واحدة، وكذلك الأمر في الحالة C حيث يظهر الشكل (5-15) انخفاض إضافي في الإنتاجية عن الحالة الأولى وذلك نتيجة تطبيق هجوم تعاوني بعقدتين خبيثتين تعملان معاً، ولكن بالرغم من ذلك لم يتم الحصول على سلوك واضح للبروتوكول AODV من هذه الحالة الفردية فقط، ولذلك تم حساب بارامتر متوسط الإنتاجية والذي يعطي فكرة أكثر وضوحاً وشمولية ويتم ذلك من خلال تغيير كثافة الشبكة للحصول على شبكة بإحجام مختلفة صغيرة ومتوسطة وكبيرة من حيث عدد العقد المكونة لها، وذلك ضمن نفس مساحة العمل والمحددة بـ 1186m * 584m، مع تغيير في عدد العقد المشتركة بالهجوم التعاوني حيث تتحول كل من المخططات السابقة إلى نقطة واحدة فقط، وتم توضيح ذلك في السيناريوهين التاليين الثاني والثالث.

السيناريو الثاني:

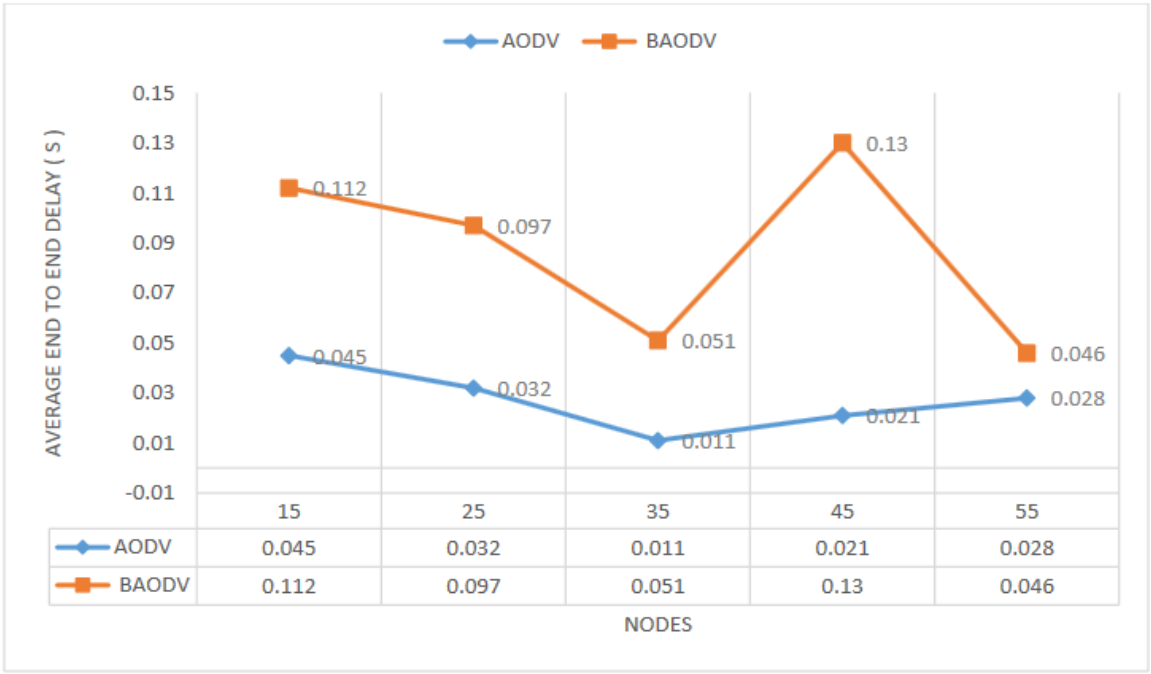
تبيّن لنا من خلال السيناريو الأول أنه لا يمكن الحصول على توصيف دقيق لإداء الشبكة العاملة مع البروتوكول AODV والتي تمت مهاجمتها بهجوم الثقب الأسود لذلك تم الانتقال في السيناريو الثاني إلى قياس بارامتر متوسط الإنتاجية Average Throughput، بالإضافة لقياس التأخير الزمني نهاية إلى نهاية End-To-end Delay (ETD)، ومعدل توصيل الرزم ضمن الشبكة Packet Delivery Rate (PDR) والذي يُحسَب كنسبة مئوية، وذلك ضمن شبكة ذات أحجام كبيرة وصغيرة ومتوسطة بكثافة عقد متغيرة من 15 عقدة وحتى 55 عقدة، مع وجود هجوم ثقب أسود تعاوني مكون من 4 عقد خبيثة متوزعة ضمن الشبكة، وتمت المحاكاة مع وجود حركية للعقد بنوعيها النظامية والخبيثة ضمن الشبكة وبسرعة ثابتة 40 متر بالثانية وذلك ضمن مساحة شبكة 584*1186 متر مربع، ومدى الأرسال للعقد محدد ب 250 متر، مع تفعيل تطبيق نقل بيانات CBR يعمل مع وكيل النقل UDP بمعدل بيانات 2 Mb بحيث يحقق حمل نقل بيانات كبير نوعاً ما ضمن الشبكة، وكانت النتائج كما يلي:



الشكل(5-16) متوسط الإنتاجية Average Throughput مع تغير كثافة الشبكة



الشكل(5-17) معدل وصول الرزم PDR مع تغير كثافة الشبكة



الشكل(5-18) التأخير الزمني الكلي ETD مع تغير كثافة الشبكة

يتبين لنا من ملاحظة الشكلين (5-16) و (5-17) انخفاض في الإنتاجية Throughput ومعدل توصيل الرزم Packet Delivery Rate (PDR) وذلك شبكة ذات كثافة متغيرة من 15 وحتى 55 عقدة في ظل وجود هجوم ثقب أسود تعاوني بعدد ثابت من العقد الخبيثة (محدد بأربع عقد مهاجمة) وذلك من خلال مراقبة تغير الخط البياني للبروتوكول BAODV المُعبِر عن سلوك الشبكة عند تطبيق هجوم الثقب التعاوني.

حيث نلاحظ من الشكلين السابقين أن زيادة عدد العقد ضمن الشبكة (كثافة الشبكة) يؤدي إلى تقليل تأثير الهجوم وذلك حتى حد معين لكثافة الشبكة 35 عقدة وذلك تبعاً لزيادة عمليات الإرسال والاستقبال وتوفر مسارات إضافية بديلة لمرور رزم البيانات تؤدي إلى تقلل تأثير العقد المهاجمة.

وبعد ذلك تنخفض الإنتاجية ومعدل توصيل الرزم بشكل واضح، وذلك بسبب أن الكثافة العالية للعقد تؤدي إلى حصول ازدحام وهذا يزيد عدد مرات إعادة الارسال واسقاط الرزم وبالتالي ينخفض أداء الشبكة عند كثافة عقد 45 عقدة وما فوق عند عدم وجود هجوم (البروتوكول AODV)، ونلاحظ عند كثافة شبكة 45 عقدة في حالة وجود هجوم (البروتوكول BAODV) زيادة تأثير الهجوم (انخفاض إضافي في الإنتاجية ومعدل الوصول) ويُفسَر ذلك بأن كل عقدة مهاجمة تؤثر على عدد أكبر من العقد نتيجة الكثافة العالية لعقد الشبكة في نفس مساحة العمل المحددة.

يتبين لنا أيضاً من خلال ملاحظة الشكل (5-18) المُعبِر عن التأخير الزمني الكلي End-To-end Delay (ETD) أن تطبيق خوارزمية الهجوم التعاوني BAODV تؤدي إلى زيادة التأخير الزمني بنسبة كبيرة، وتتفاوت هذه الزيادة في التأخير تبعاً لتغير كثافة الشبكة وتغير مواقع العقد ضمن كل كثافة وذلك نظراً لوجود حركية للعقد ضمن الشبكة بسرعة ثابتة 40 متر في الثانية.

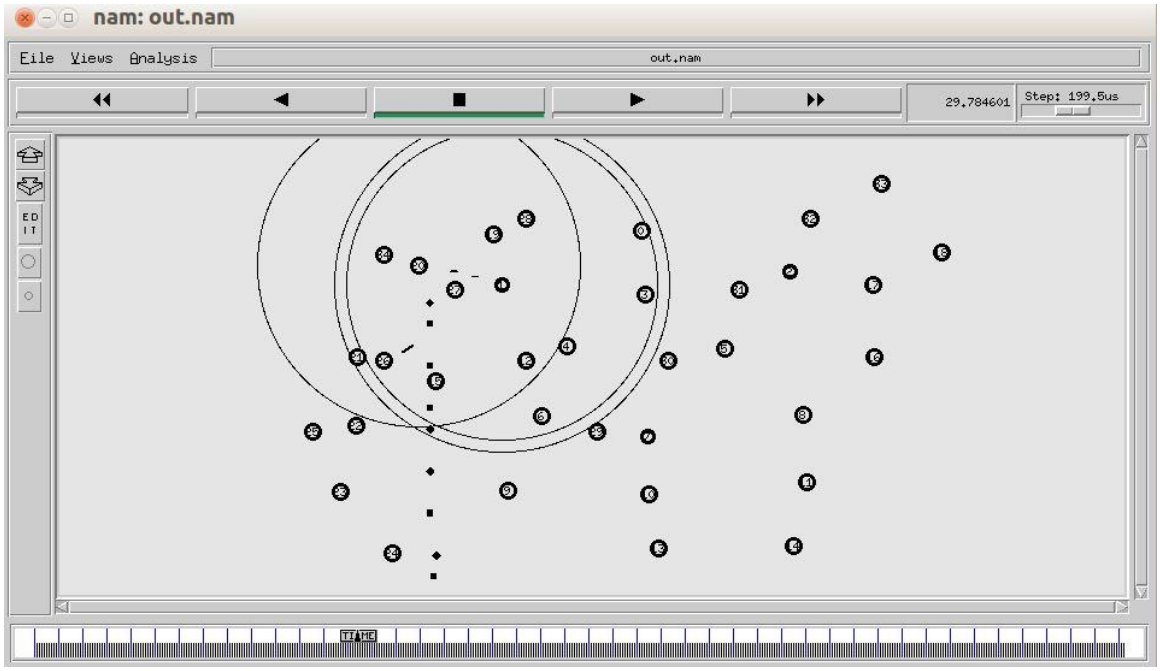
ويُفسَر ذلك بأن هذا البارامتر يعبر عن الزمن التي تستغرقه رزمة البيانات حتى تصل إلى وجهتها النهائية، وبما أن الهجوم يعمل على اسقاط الرزم ومنعها من الوصول لوجهتها النهائية قدر الإمكان وبالتالي هذا ما يؤدي إلى زيادة عدد عمليات إعادة الإرسال وبالتي زيادة في التأخير الزمني (تأخير العبور أو الانتشار Propagation Delay PD)، فضلاً عن التأخير الناتج عن حالات الازدحام الناتجة عن الكثافة العالية والحركية التي تؤدي أحياناً إلى تركز العقد ضمن منطقة محددة وهذا ما ينتج عنه استهلاك عرض الحزمة المحدودة وبالتالي زيادة في اسقاط الرزم وعمليات إعادة الإرسال ويتجلى ذلك بشكل واضح عن كثافة الشبكة 45 عقدة في البروتوكول BAODV.

نلاحظ من النتائج في هذا السيناريو أن أفضل حالة لإداء الشبكة كانت ضمن كثافة شبكة 35 عقدة حيث حصلنا على أعلى قيمة للإنتاجية ولمعدل وصول البيانات وحصلنا أيضاً على أقل قيمة للتأخير الزمني لذلك تم الانتقال إلى دراسة هذه الحالة بالتفصيل في ظل تغير عدد العقد الخبيثة المشتركة بالهجوم وتم توثيق العمل في السيناريو التالي.

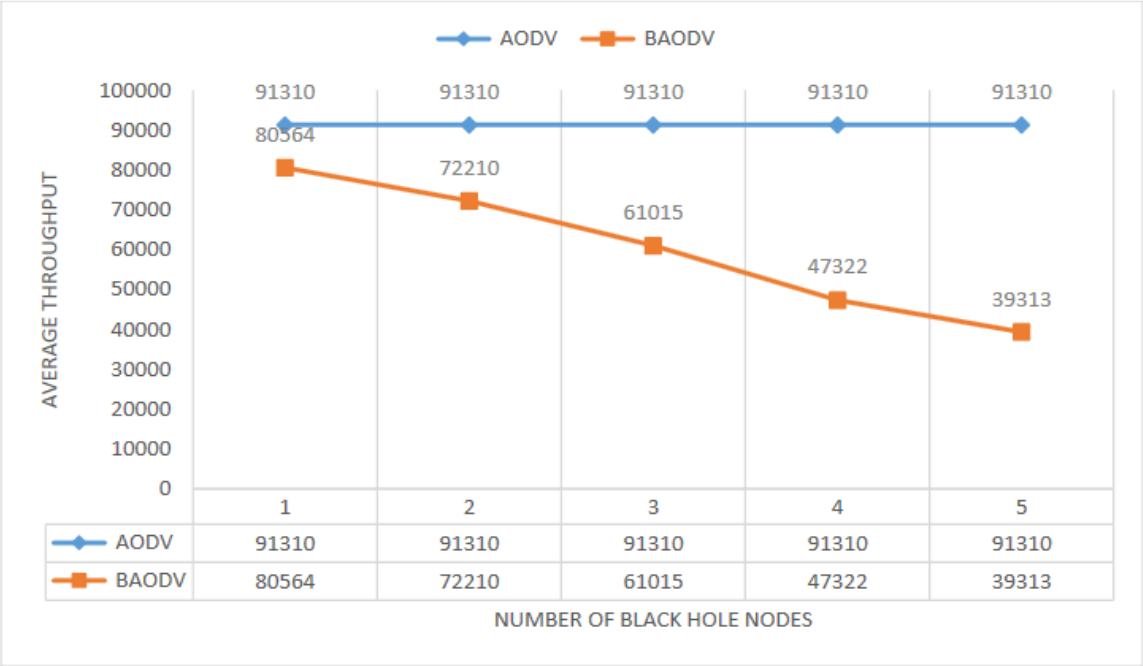
السيناريو الثالث:

تم في هذا السيناريو دراسة شبكة بكثافة 35 عقدة مع تغير عدد العقد المشكلة لهجوم الثقب الأسود، بدءً من هجوم ثقب أسود فردي Single Black Hole بعقدة خبيثة واحدة فقط ووصولاً إلى هجوم ثقب أسود تعاوني Cooperative Black Hole مكون من خمس عقد خبيثة وذلك ضمن شبكة بتوزع عقد عشوائي مع وجود حركية للعقد بسرعة ثابتة تعادل 40 متر في الثانية، وتم اختيار هذه الكثافة بناءً على فعالية أداء بروتوكول التوجيه عندها بغية مراقبة تأثير خوارزمية الهجوم على هذه الحالة، وتم قياس بارامترات الإنتاجية Throughput، ومعدل وصول الرزم PDR، والتأخير الزمني الكلي ETD، وكانت النتائج كما يلي:

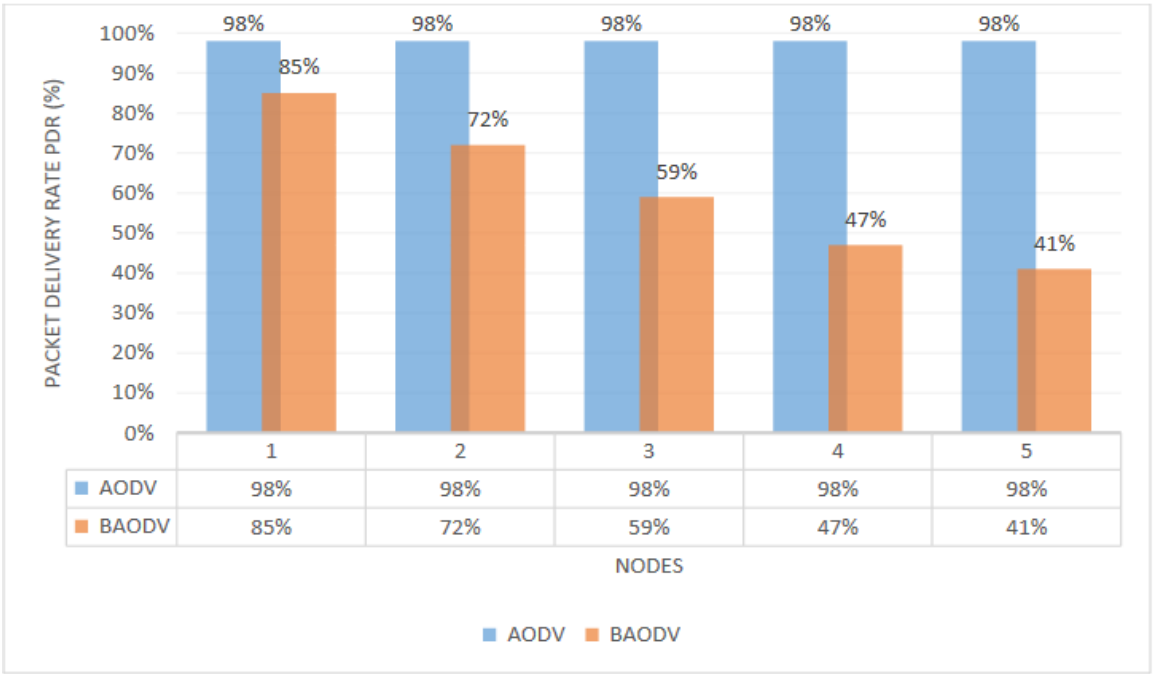
تظهر نافذة الخرج في برنامج الـ NAM عملية إسقاط الرزم من قبل العقدة المهاجمة 20 وذلك في اللحظة الزمنية 29.7 ثانية ومنعها من الوصول إلى وجهتها كما يوضح الشكل (5-19):



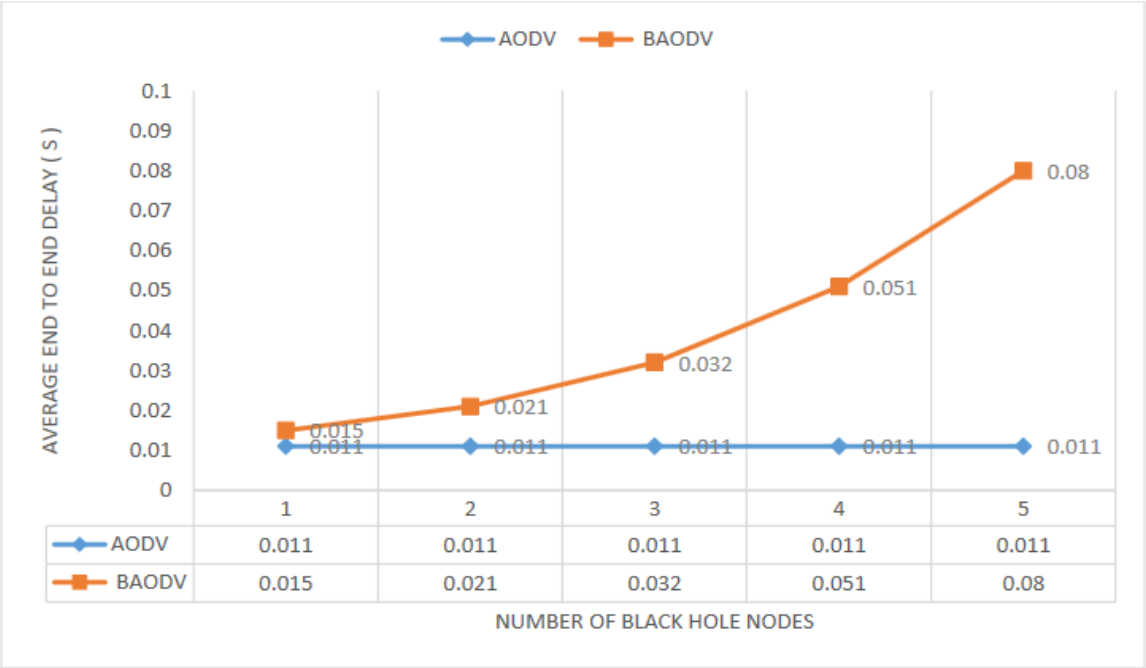
الشكل (5-19) خرج برنامج NAM في اللحظة 29 ثانية لشبكة مكونة من 35 عقدة بعقدة خبيثة رقم 20



الشكل(5-20) متوسط الإنتاجية Average Throughput ضمن كثافة ثابتة 35 عقدة، مع تغير عدد العقد الخبيثة



الشكل(5-21) معدل وصول الرزم PDR ضمن كثافة ثابتة 35 عقدة، مع تغير عدد العقد الخبيثة



الشكل(5-22) التأخير الزمني الكلي ETD ضمن كثافة ثابتة 35 عقدة، مع تغير عدد العقد الخبيثة

يتبين لنا من ملاحظة الشكلين (5-20) و (5-21) أن زيادة عدد العقد الخبيثة ضمن الشبكة يؤدي بشكل واضح إلى زيادة فعالية هجوم الثقب الأسود التعاوني حيث يستمر بارامترا الإنتاجية Throughput ومعدل وصول الرزم PDR بالانخفاض مع هذه الزيادة في عدد المهاجمين، ويُفسَر هذا الانخفاض بأن هجوم الثقب الأسود التعاوني أكثر فعالية وأشد تعقيداً من هجوم الثقب الأسود المنفرد.

حيث تُعطى علاقة الإنتاجية كما ذكرنا سابقاً كما يلي: $\frac{\text{حجم البيانات المستقبلة بشكل صحيح}}{\text{الزمن}}$، ويتم حسابها بعدد البايتات في الثانية (Bytes/sec)، وتعطى أيضاً علاقة معدل وصول الرزم كما يلي: $\frac{\text{عدد الرزم المستقبلة}}{\text{عدد الرزم المرسلة}}$، ويتم حسابها كنسبة مئوية كما ورد سابقاً، بما أن الهجوم يقوم بحذف رزم البيانات فلن تصل كل الرزم إلى أهدافها، مما يؤدي إلى انخفاض حجم الرزم المستقبلة، وبالتالي تنخفض الإنتاجية ومعدل وصول الرزم وفق العلاقتين السابقتين، وعند عند زيادة عدد العقد المهاجمة تزداد فعالية الهجوم، أي يقل عدد الرزم التي تصل إلى أهدافها، فينخفض حجم البيانات المُستقبَلة مع كل زيادة في عدد العقد المهاجمة وبالتالي يقل أداء الشبكة تدريجياً.

يتبين لنا أيضاً من خلال ملاحظة الشكل (5-22) المُعبِر عن التأخير الزمني الكلي End-To-end Delay (ETD) أن تأثير خوارزمية هجوم الثقب الأسود (BAODV) التعاوني يزداد مع زيادة عدد المهاجمين، أي أن التأخير الزمني يتناسب طرداً مع زيادة عدد المهاجمين ضمن الشبكة ويُفسَر ذلك بإن زيادة عدد المهاجمين سوف يؤدي حكماً إلى زيادة عمليات إسقاط الرزم ضمن الشبكة وبالتالي تزداد عمليات إعادة الإرسال ويزداد الزمن اللازم لوصول الرزم إلى وجهتها وبالتالي ينخفض أداء الشبكة.

5-8 الخاتمة والآفاق المستقبلية:

تعد بروتوكولات التوجيه العنصر الأهم وحجر الأساس في شبكات MANETs لأن العقد بكل بساطة مضطرة للاعتماد على بعضها البعض بشكل كامل لتحقيق اتصالية الشبكة وضمان استمرار هذه الاتصالية حيث أن البنية التحتية تغيب تماماً في هذا النوع من الشبكات، لذلك كانت هذه الشبكات هدفاً كبيراً للهجمات الأمنية التي تحول دون وصول البيانات إلى أهدافها، أو تتنصت على محتوى الرسائل المتبادلة وتحصل على نسخه منها.

وبما وسط الاتصال اللاسلكي يعتبر وسط محدود الأمن الفيزيائي لذلك كان تحقيق موثوقية وخصوصية الاتصال في هذه الشبكات تحدياً أمنياً كبيراً ومستمراً، وإن أهم هذه التحديات والهجمات التي تستهدف عملية التوجيه وتسيير الرزم هي هجمات الثقوب، وقد طُرِحت العديد من الحلول لتجنب تأثير هذه المشكلة على عمل الشبكة ولكن هذه الحلول كانت في أغلب الأحيان حلول مقتصرة على حالات خاصة جداً ومحدودة لإشكال هذا الهجوم، وبناءً على ذلك تم في هذا البحث دارسة هجوم الثقب الأسود بنوعية الفردي Single Black Hole Attack والتعاوني Cooperative Black Hole Attack وذلك ضمن شروط عمل واقعية لشبكة ديناميكية تحوي حركية للعقد مع مراعاة تغير كثافة هذه الشبكة من شبكة صغيرة إلى متوسطة ووصولاً إلى شبكة كبيرة من حيث عدد العقد العاملة ضمن مساحة عمل محددة، وأيضاً تم الأخذ بالحسبان وجود عدة عقد مهاجمة تشترك في تنفيذ هذا الهجوم بغية التأثير على الشبكة المعادية قدر الإمكان.

وتبين لنا من خلال الدراسة والمحاكاة أن هجوم الثقب الأسود يؤثر بشكل واضح على معدل نقل البيانات في شبكات MANETs العاملة مع بروتوكول التوجيه التفاعلي AODV وذلك من خلال مراقبة بارامترات الإنتاجية ومعدل وصول الرزم والتأخير الزمني، وتبين لنا أيضاً أن هجوم الثقب الأسود التعاوني أكثر فعاليةً وأشد تأثيراً من هجوم الثقب الأسود الفردي، حيث تتناسب فعالية الهجوم طرداً مع زيادة عدد المهاجمين.

تتغير فعالية هجوم الثقب الأسود التعاوني تبعاً لتغير كثافة الشبكة وتغير مواقع العقد المهاجمة وذلك تحت تأثير عدد ثابت من المهاجمين.

وأيضاً تتغير فعالية الهجوم التعاوني في ظل كثافة ثابتة للشبكة تبعاً للتغيرات السريعة في بنية الشبكة نتيجة حركة العقد، وتبعاً لتغير عدد العقد المهاجمة الأمر الذي يؤثر بشكل كبير على معدل نقل البيانات.

ويبقى البحث في هذا المجال مفتوحاً باعتبار وجود طلب متزايد باستمرار على هذا النوع من الشبكات، ويوصى في المستقبل بدراسة هجوم الثقب الأسود بنوعيه الفردي والتعاوني مع بروتوكول توجيه أخر مثل البروتوكول OLSR أو البروتوكول DSR أو أحد البروتوكولات الهجينة.

ويوصى أيضاً بدراسة تأثير حركة العقد المهاجمة بسرعات مختلفة على أداء الشبكة في ظل وجود هجوم الثقب الأسود مع البروتوكول AODV ضمن نفس حجم الشبكة الحالي، مع الأخذ بالحسبان موضوع طاقة العقد لأنه بارامتر مهم جداً ومحدود في أغلب شبكات MANETs.

بالإضافة إلى ذلك فإن أي حل مقترح لتفادي هذا الهجوم يجب أن يأخذ بالحسبان بيئة وظروف العمل الحقيقية لهذه الشبكات وحركتها وطبيعتها الديناميكية، وأن تكون التكلفة الناتجة عن تطبيق هذا الحل في حدودها الدنيا بحيث يقترب أداء خوارزمية الحل قدر الإمكان من أداء الحالة الطبيعية لخوارزمية عمل بروتوكول التسيير المستخدم.

5-9 المراجع:

[1] Mohapatra, P., & Krishnamurthy, S. (Eds.). (2004). *AD HOC NETWORKS: technologies and protocols*. Springer Science & Business Media.

[2] Khattak, H. (2013, September). A hybrid approach for preventing Black and Gray hole attacks in MANET. In *Eighth International Conference on Digital Information Management (ICDIM 2013)* (pp. 55-57). IEEE.

[3] Deshmukh, S. R., & Chatur, P. N. (2016, March). Secure routing to avoid black hole affected routes in MANET. In *2016 Symposium on Colossal Data Analysis and Networking (CDAN)* (pp. 1-4). IEEE.

[4] Rathiga, P., & Sathappan, S. (2016, October). Hybrid detection of Black hole and gray hole attacks in MANET. In *2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)* (pp. 135-140). IEEE.

[5] Sharma, N., & Bisen, A. S. (2016, March). Detection as well as removal of black hole and gray hole attack in MANET. In *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)* (pp. 3736-3739). IEEE.

[6] Thakker, J., Desai, J., & Ragha, L. (2016, March). Avoidance of co-operative black hole attack in AODV in MANET. In *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)* (pp. 1049-1053). IEEE.

[7] Nitnaware, D., & Thakur, A. (2016, February). Black hole attack detection and prevention strategy in DYMO for MANET. In *2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN)* (pp. 279-284). IEEE.

[8] Saurabh, V. K., Sharma, R., Itare, R., & Singh, U. (2017, April). Cluster-based technique for detection and prevention of black-hole attack in MANETs. In *2017 International conference of Electronics, Communication and Aerospace Technology (ICECA)* (Vol. 2, pp. 489-494). IEEE.

[9] Dhende, S., Musale, S., Shirbahadurkar, S., & Najan, A. (2017, March). SAODV: Black hole and gray hole attack detection protocol in MANETs. In *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)* (pp. 2391-2394). IEEE.

[10] Panda, N., & Pattanayak, B. K. (2018). Energy aware detection and prevention of black hole attack in MANET. *International Journal of Engineering and Technology (UAE), 7*(2.6), 135-140.

[11] Gurung, S., & Chauhan, S. (2019). A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET. *Wireless Networks*, *25*(4), 1685-1695.

[12] Baugh, J. P. (2007). *Establishing Security and Privacy in Vehicular Ad Hoc Networks Via Utilization of Group Signatures*. University of Michigan-Dearborn.

[13] Wang, L., Wu, K., & Hamdi, M. (2012). Combating hidden and exposed terminal problems in wireless networks. *IEEE Transactions on Wireless Communications*, *11*(11), 4204-4213.

[14] Devangavi, A. D., & Gupta, R. (2017, August). Routing protocols in VANET—A survey. In *2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon)* (pp. 163−167). IEEE.

[15] Fahmy, H. M. A. (2020). *Wireless sensor networks*. Springer International Publishing.

[16] Rezazadeh, J., Moradi, M., Ismail, A. S., & Dutkiewicz, E. (2014). Superior path planning mechanism for mobile beacon-assisted localization in wireless sensor networks. *IEEE Sensors Journal*, *14*(9), 3052-3064.

[17] Reddy, V. B., Negi, A., & Venkataraman, S. (2016, February). A comparison of trust in MANETs and WSNs. In *2016 IEEE 6th International Conference on Advanced Computing (IACC)* (pp. 577-581). IEEE.

[18] Kim, Y. K., Wang, H., & Mahmud, M. S. (2016). Wearable body sensor network for health care applications. In *Smart Textiles and Their Applications* (pp. 161-184). Woodhead Publishing.

[19] Sarkar, S. K., Basavaraju, T. G., & Puttamadappa, C. (2007). *Ad hoc mobile wireless networks: principles, protocols and applications*. CRC Press.

[20] Cheng, X., Huang, X., & Du, D. Z. (Eds.). (2013). *Ad hoc wireless networking* (Vol. 14). Springer Science & Business Media.

[21] O'hara, B., & Petrick, A. (2005). *IEEE 802.11 handbook: a designer's companion*. IEEE Standards Association.

[22] Byeon, S., Yang, C., Lee, O., Yoon, K., & Choi, S. (2015, June). Enhancement of wide bandwidth operation in IEEE 802.11 ac networks. In *2015 IEEE International Conference on Communications (ICC)* (pp. 1547-1552). IEEE.

[23] Shenbagapriya, R., & Kumar, N. (2014, November). A survey on proactive routing protocols in MANETs. In *2014 International Conference on Science Engineering and Management Research (ICSEMR)* (pp. 1-7). IEEE.

[24] Patel, D. N., Patel, S. B., Kothadiya, H. R., Jethwa, P. D., & Jhaveri, R. H. (2014, February). A survey of reactive routing protocols in MANET. In *International Conference on Information Communication and Embedded Systems (ICICES2014)* (pp. 1-6). IEEE.

[25] Raheja, K., & Maakar, S. K. (2014). A survey on different hybrid routing protocols of MANET. *IJCSIT) International Journal of Computer Science and Information Technologies*, *5*(4), 5512-5516.

[26] Bidabadi, A. (2006). Cross-layer optimization of ad hoc on-demand distance vector routing protocol.

[27] Jiang, F., & Hao, J. (2010, February). Simulation of an improved AODV algorithm for ad hoc network. In *2010 The 2nd International Conference on Computer and Automation Engineering (ICCAE)* (Vol. 1, pp. 540-543). IEEE.

[28] Perkins, C., Belding-Royer, E., & Das, S. (2003). Ad hoc on-demand distance vector (AODV) routing.

[29] Razak, S. A., Furnell, S. M., & Brooke, P. J. (2004, June). Attacks against mobile ad hoc networks routing protocols. In *Proceedings of 5th annual postgraduate symposium on the convergence of telecommunications, Networking & Broadcasting, PGNET* (Vol. 2004).

[30] Buttyan, L., & Hubaux, J. P. (2007). *Security and cooperation in wireless networks: thwarting malicious and selfish behavior in the age of ubiquitous computing*. Cambridge University Press.

[31] Wu, B., Chen, J., Wu, J., & Cardei, M. (2007). A survey of attacks and countermeasures in mobile ad hoc networks. In *Wireless network security* (pp. 103-135). Springer, Boston, MA.

[32] Bala, A., Kumari, R., & Singh, J. (2010). Investigation of Blackhole Attack on AODV in MANET. *journal of emerging technologies in web intelligence*, *2*(2), 96-100.

[33] Gorlatova, M. A. (2006). *Review of existing wormhole attack discovery techniques*. OTTAWA UNIV (ONTARIO) SCHOOL OF INFORMATION TECHNOLOGY.

[34] Gurung, S., & Saluja, K. K. (2014). Mitigating impact of blackhole attack in MANET. In *Int. Conf. on Recent Trends in Information, Telecommunication and Computing, ITC*.

6 الفصل السادس

الملحقات

1-6 ملحق A: الرّماز المصدري المكتوب بلغة TCI لتعريف طوبولوجيا الشبكة:

```
# This script is created by NSG2 beta1
# <http://wushoupong.googlepages.com/nsg>

#===================================
#     Simulation parameters setup
#===================================
set val(chan)   Channel/WirelessChannel    ;# channel type
set val(prop)   Propagation/TwoRayGround   ;# radio-
propagation model
set val(netif)  Phy/WirelessPhy            ;# network
interface type
set val(mac)    Mac/802_11                 ;# MAC type
set val(ifq)    Queue/DropTail/PriQueue    ;# interface
queue type
set val(ll)     LL                         ;# link layer
type
set val(ant)    Antenna/OmniAntenna        ;# antenna model
set val(ifqlen) 50                         ;# max packet in
ifq
set val(nn)     55                         ;# number of
mobilenodes
set val(rp)     BAODV                      ;# routing
protocol
set val(x)      1186                      ;# X dimension of
topography
set val(y)      584                      ;# Y dimension of
topography
set val(stop)   100.0                        ;# time of
simulation end
set val(t1)     0.0                         ;
set val(t2)     0.0                          ;

#===================================
#        Initialization
#===================================
#Create a ns simulator
set ns [new Simulator]

#Setup topography object
set topo       [new Topography]
$topo load_flatgrid $val(x) $val(y)
create-god $val(nn)
#Open the NS trace file
set tracefile [open out.tr w]
```

```
$ns trace-all $tracefile
#Open the NAM trace file
set namfile [open out.nam w]
$ns namtrace-all $namfile
$ns namtrace-all-wireless $namfile $val(x) $val(y)
set chan [new $val(chan)];#Create wireless channel

#===================================
#     Mobile node parameter setup
#===================================
$ns node-config -adhocRouting  $val(rp) \
                -llType        $val(ll) \
                -macType       $val(mac) \
                -ifqType       $val(ifq) \
                -ifqLen        $val(ifqlen) \
                -antType       $val(ant) \
                -propType      $val(prop) \
                -phyType       $val(netif) \
                -channel       $chan \
                -topoInstance  $topo \
                -agentTrace    ON \
                -routerTrace   ON \
                -macTrace      ON \
                -movementTrace ON

#===================================
#        Generate movement
#===================================
$ns at 0 " $n6 setdest 1086 453 40 "
$ns at 10 " $n18 setdest 877 39 40 "
$ns at 20 " $n18 setdest 500 117 40 "
$ns at 60 " $n18 setdest 400 100 40 "
$ns at 60 " $n18 setdest 340 430 40 "
$ns at 40 " $n6 setdest 400 500 40 "
$ns at 10 " $n15 setdest 650 470 40 "
$ns at 10 " $n5 setdest 550 220 40 "

#malicoius node attackers
$ns at 0.0 "[$n6 set ragent_] hacker"
$ns at 0.0 "[$n8 set ragent_] hacker"
$ns at 0.0 "[$n20 set ragent_] hacker"

#===================================
#        Agents Definition
#===================================
#===================================
#        Applications Definition
```

```
#====================================
#Setup a UDP connection
set udp0 [new Agent/UDP]
$ns attach-agent $n21 $udp0
set null1 [new Agent/Null]
$ns attach-agent $n18 $null1
$ns connect $udp0 $null1
$udp0 set packetSize_ 1500
#Setup a CBR Application over UDP connection
set cbr0 [new Application/Traffic/CBR]
$cbr0 attach-agent $udp0
$cbr0 set packetSize_ 1500
$cbr0 set rate_ 2Mb
$cbr0 set random_ null
$ns at 1.0 "$cbr0 start"
$ns at 20.0 "$cbr0 stop"

#Setup a UDP connection
set udp1 [new Agent/UDP]
$ns attach-agent $n14 $udp1
set null2 [new Agent/Null]
$ns attach-agent $n18 $null2
$ns connect $udp1 $null1
$udp1 set packetSize_ 1500

#Setup a CBR Application over UDP connection
set cbr1 [new Application/Traffic/CBR]
$cbr1 attach-agent $udp1
$cbr1 set packetSize_ 1500
$cbr1 set rate_ 2Mb
$cbr1 set random_ null
$ns at 20.0 "$cbr1 start"
$ns at 40.0 "$cbr1 stop"

#Setup a UDP connection
set udp3 [new Agent/UDP]
$ns attach-agent $n22 $udp3
set null3 [new Agent/Null]
$ns attach-agent $n18 $null3
$ns connect $udp3 $null1
$udp3 set packetSize_ 1500

#Setup a CBR Application over UDP connection
set cbr4 [new Application/Traffic/CBR]
$cbr4 attach-agent $udp4
$cbr4 set packetSize_ 1500
$cbr4 set rate_ 2Mb
```

```
$cbr4 set random_ null
$ns at 60.0 "$cbr4 start"
$ns at 80.0 "$cbr4 stop"
set udp5 [new Agent/UDP]
$ns attach-agent $n16 $udp5
set null5 [new Agent/Null]
$ns attach-agent $n18 $null5
$ns connect $udp5 $null5
$udp5 set packetSize_ 1500

#Setup a CBR Application over UDP connection
set cbr5 [new Application/Traffic/CBR]
$cbr5 attach-agent $udp5
$cbr5 set packetSize_ 1500
$cbr5 set rate_ 2Mb
$cbr5 set random_ null
$ns at 80.0 "$cbr5 start"
$ns at 100.0 "$cbr5 stop"

#====================================
#        Termination
#====================================
#Define a 'finish' procedure
proc finish {} {
    global ns tracefile namfile
    $ns flush-trace
    close $tracefile
    close $namfile
 exec perl throughput.pl out.tr _18_ 2 > thp3.tr
exec xgraph thp3.tr
exec awk -f avgStats.awk src=8 dst=18 flow=1 pkt=1500
out.tr > avgTCP.out
    exec nam out.nam &
    exit 0
}
for {set i 0} {$i < $val(nn) } { incr i } {
    $ns at $val(stop) "\$n$i reset"
}
$ns at $val(stop) "$ns nam-end-wireless $val(stop)"
$ns at $val(stop) "finish"
$ns at $val(stop) "puts \"done\" ; $ns halt"
$ns run
```

2-6 ملحق B: جزء من الكود البرمجي بلغة C++ للخوارزمية المُعدلة BAODV:

```
AODV::command(intargc, const char*const* argv) {
if(argc == 2) {
Tcl&tcl = Tcl::instance();

if(strncasecmp(argv[1], "id", 2) == 0) {
tcl.resultf("%d", index);
return TCL_OK;
    }
                    if(strcmp(argv[1], "blackhole1") == 0) {
     malicious1= index;
          printf("malicious %d", malicious1);
return TCL_OK;
    }
                    if(strcmp(argv[1], "blackhole2") == 0) {
malicious2=index;
                              printf("malicious %d",
malicious2);
return TCL_OK;
    }
                    if(strcmp(argv[1], "blackhole3") == 0) {
                              malicious3= index;
printf("malicious %d", malicious3);
return TCL_OK;
    }

AODV::AODV(nsaddr_t id) : Agent(PT_AODV),
btimer(this), htimer(this), ntimer(this),
rtimer(this), lrtimer(this), rqueue() {
index = id;
seqno = 2;
bid = 1;
  LIST_INIT(&nbhead);
  LIST_INIT(&bihead);
malicious1=999;
  malicious2=999;
  malicious3=999;

   //add in receive route request

if(rq->rq_dst == index) {

#ifdef DEBUG
fprintf(stderr, "%d - %s: destination sending reply\n",
index, __FUNCTION__);
```

```
#endif // DEBUG


   // Just to be safe, I use the max. Somebody may have
   // incremented the dstseqno.
seqno = max(seqno, rq->rq_dst_seqno)+1;
if (seqno%2) seqno++;

sendReply(rq->rq_src,           // IP Destination
              1,                   // Hop Count
index,                  // Dest IP Address
seqno,                  // Dest Sequence Num
              MY_ROUTE_TIMEOUT,     // Lifetime
rq->rq_timestamp);    // timestamp

   Packet::free(p);
 }
 //blackhole attackers

else if(index==malicious1)
 {
seqno = max(seqno, rq->rq_dst_seqno)+1;
if (seqno%2) seqno++;

sendReply(rq->rq_src,           // IP Destination
              1,                   // Hop Count
rq->rq_dst,
                              seqno,
                               MY_ROUTE_TIMEOUT,
rq->rq_timestamp);    // timestamp
 //rt->pc_insert(rt0->rt_nexthop);
   Packet::free(p);
 }
else if(index==malicious2)
 {
seqno = max(seqno, rq->rq_dst_seqno)+1;
if (seqno%2) seqno++;

sendReply(rq->rq_src,           // IP Destination
              1,                   // Hop Count
rq->rq_dst,
                              seqno,
                               MY_ROUTE_TIMEOUT,
rq->rq_timestamp);    // timestamp
 //rt->pc_insert(rt0->rt_nexthop);
   Packet::free(p);
 }
```

```
else if(index==malicious3)
 {
seqno = max(seqno, rq->rq_dst_seqno)+1;
if (seqno%2) seqno++;

sendReply(rq->rq_src,           // IP Destination
              1,                   // Hop Count
rq->rq_dst,
                                seqno,
                                 MY_ROUTE_TIMEOUT,
rq->rq_timestamp);    // timestamp
 //rt->pc_insert(rt0->rt_nexthop);
   Packet::free(p);
 }


 // add in route resolve function (AODV::rt_resolve(Packet
*p) )
else {
 Packet *rerr = Packet::alloc();
structhdr_aodv_error *re = HDR_AODV_ERROR(rerr);
 /*
  * For now, drop the packet and send error upstream.
  * Now the route errors are broadcast to upstream
  * neighbors - Mahesh 09/11/99
  */

assert (rt->rt_flags == RTF_DOWN);
re->DestCount = 0;
re->unreachable_dst[re->DestCount] = rt->rt_dst;
re->unreachable_dst_seqno[re->DestCount] = rt->rt_seqno;
re->DestCount += 1;
#ifdef DEBUG
fprintf(stderr, "%s: sending RERR...\n", __FUNCTION__);
#endif
if((index==malicious1)||(index==malicious2)||
(index==malicious3));
else
sendError(rerr, false);

drop(p, DROP_RTR_NO_ROUTE);
```

4-6 ملحق C: الرّمازات المصدرية المكتوبة بلغة C++ لحساب النتائج:

- حساب الإنتاجية **Throughput**:

```
# type: perl throughput.pl <trace file> <required node>
<granlarity>   >    output file
$infile=$ARGV[0];
$tonode=$ARGV[1];
$granularity=$ARGV[2];
#we compute how many bytes were transmitted during time
interval specified
#by granularity parameter in seconds
$sum=0;
$clock=0;
      open (DATA,"<$infile")
        || die "Can't open $infile $!";

    while (<DATA>) {
            @x = split(' ');
#column 1 is time
if ($x[1]-$clock <= $granularity)
{
#checking if the event corresponds to a reception
if ($x[0] eq 'r')
{
#checking if the destination corresponds to arg 1
#checking if the packet type is TCP
if ($x[6] eq 'udp')
{
    $sum=$sum+$x[7];
}}}
else
{   $throughput=$sum/$granularity;
    print STDOUT "$x[1] $throughput\n";
    $clock=$clock+$granularity;    $sum=0;
}}
   $throughput=$sum/$granularity;
    print STDOUT "$x[1] $sum $throughput\n";
    $clock=$clock+$granularity;
    $sum=0;
    close DATA;
 #Average Throughput
$avr= $sum/50;
print STDOUT "$avr \n";
  exit(0);
```

- حساب معدل وصول الرزم PDR:

```
#we compute how many bytes were transmitted during time
interval specified
#by granularity parameter in seconds
$infile=$ARGV[0];
$dnode=$ARGV[1];
$scount=0;
$rcount=0;
$pdr=0;
$clock=0;
      open (DATA,"<$infile")
        || die "Can't open $infile $!";
    while (<DATA>) {
              @x = split(' ');

#column 1 is time
#checking if the event corresponds to a reception
if ($x[0] eq 's')
{
if ($x[3] eq 'MAC')
{
#checking if the destination corresponds to arg 1
if (($x[10] eq $dnode) )
{
#checking if the packet type is TCP
if ($x[6] eq 'cbr')
{ $scount=$scount+1;
}}}}
if ($x[0] eq 'r')
{
if ($x[3] eq 'MAC')
{
#checking if the destination corresponds to arg 1
if ($x[10] eq $dnode) #change according to your destination
node
{
#checking if the packet type is TCP
if ($x[6] eq 'cbr')
{ $rcount=$rcount+1;
}}}}}
   $pdr=$rcount/$scount;
    print STDOUT "PDR $pdr \n scount $scount rcount
$rcount\n";
      $rcount=0;
    close DATA;
exit(0);
```

- حساب التأخير الزمني ETD:

```
BEGIN{
recvdSize =0
startTime =1e6
stopTime =0
for (i in send{ )
send[i] = 0
}
for (i in recv{ )
recv[i] = 0
}
delay = avg_delay = num = 0
} {
# Trace line format: normal
#if ($2 != "-t{ )"
#event = $1
#time = $2
#if (event == "+" || event == "-") node_id = $3
#if (event == "r" || event == "d") node_id = $4
#flow_id = $8
#pkt_id = $12
} #
# Trace line format: new
if ($2 == "-t{ )"
# field parameters of normal trace
event = $1; #; Event : r , s , d , f
time = $3; #; Time : send time , receive time ,
drop time
node = $5; #; Node : source node , receive node
trace_type = $19; #; Trace type MAC trace
pkt_id = $41; #; Event ID : Frame sequence number
for total flows
pkt_type = $35; #; Packet type : RTS , CTS , Data =
cbr , ACK
flow_id = $39;
pkt_size = $37; #; Packet size (unit : bytes )
aodv_type = $61; #; AODV_type (Request,Reply,ERROR)
}
# Store Request packets send time
if (flow_id == 0 && event == "s" && pkt_type == "cbr)"
{
if(time < startTime)
startTime =time;
send[pkt_id] = time
printf("sendPacket[%g] = %g\n",pkt_id , time)
}
# Store Reply packets arrival time
```

```
if (flow_id == 0 && event == "r" && pkt_type == "cbr)"
{if(time > stopTime)
stopTime=time;
# store packet's reception time
recv[pkt_id] = time
printf("RecvPacket [%g] = %g\n",pkt_id , time)
printf("\t\trecv[%g] = %g --> delay[%g]
=%g\n",pkt_id,time,pkt_id,recv[pkt_id]-send[pkt_id)]
print time," ",recv[pkt_id]-send[pkt_id] >
"delay_graph15.tr "
# delay+=recv[pkt_id]-send[pkt_id]
# print delay
# num;++
}
}
END{
# Compute average delay
for (i in recv{ )
if (send[i] == 0{ )
printf("\nError %g\n",i)
}
delay += recv[i] - send[i]
num++
}
# Compute average delay
print num
if (num != 0{ )
avg_delay = delay / num
} else{
avg_delay = 0
}
printf("%15s: %d\n" ,"startTime" ,startTime;)
printf("%15s: %d\n" ,"stopTime" ,stopTime;)
printf("%15s: %g\n" ,"avgDelay[ms]" ,avg_delay;)
}
```

ABSTRACT

MANETs are considered a very important wireless communication system that provides continuous services to transfer data with high efficiency in environments where there is no presence of any infrastructure (the same as destroyed infrastructure such as military networks) due to the dynamism that the nodes enjoy through establishing direct communications, and quickly adapting to the loss of any node In the network, Therefore, these networks are always subject to security challenges due to the limited physical security imposed by the nature and working conditions of this type of networks, there is a lot of research examining the effect of a single black hole attack on the AODV interactive routing protocol in networks with variable contract density.

The DOS attack was applied to MANET networks, where the effect of the black hole attack In both single and cooperative types was studied on the performance of the AODV reactive routing protocol in MANET networks within multiple scenarios for a variety of work environments in terms of network density, node traffic and number of attackers.

Keywords:

Ad-Hoc, MANETs (Mobile Ad-Hoc Networks), Black Hole Attack, Protocol (AODV), Reactive Protocols.

Syrian Arab Republic
Tartous University
Faculty of Information and
Communication Technology Engineering
Department of
Communication Technology Engineering

Increasing The Effect of The Malicious Nodes in Disabling Hostile Ad-hoc Networks

This project submitted to the Department of Communication Technology Engineering in partial fulfillment of the requirement of the MSC degree in Communication Technology Engineering

Prepared By

Mohammad Ali

Supervised BY

Dr. Eng. Naji Mohammad

Dr. Eng. Fadi Ghosna

2021